



Cellebrite  
**UFED**

## 4PC Overview guide

May 2021 | Version 7.45

## Legal notices

Copyright © 2021 Cellebrite DI Ltd. All rights reserved.

This document is delivered subject to the following conditions and restrictions:

- » This document contains proprietary information belonging to Cellebrite DI Ltd. Such information is supplied solely for the purpose of assisting explicitly and properly authorized users of the Cellebrite UFED 4PC.
- » No part of this content may be used for any other purpose, disclosed to any person or firm, or reproduced by any means, electronic or mechanical, without the express prior written permission of Cellebrite DI Ltd.
- » The text and graphics are for the purpose of illustration and reference only. The specifications on which they are based are subject to change without notice.
- » Information in this document is subject to change without notice. Corporate and individual names and data used in examples herein are fictitious unless otherwise noted.

## Warnings

**FCC WARNING:** This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions:

- 1) This device may not cause harmful interference.
- 2) This device must accept any interference received, including interference that may cause undesired operation.

# Contents

<b>1. Overview</b>	7
1.1. System requirements	8
1.2. Extraction types	9
1.3. Accessories	10
1.3.1. Cellebrite UFED Device Adapter with USB 3.0	11
1.3.2. Multi SIM Adapter	13
1.3.3. Using cables and tips	14
1.4. Supported devices	14
1.5. Cellebrite YouTube channel	15
<b>2. Getting started</b>	16
2.1. Installing Cellebrite UFED	17
2.2. Activating the license	21
2.2.1. Using a dongle license	21
2.2.2. Using a network dongle	25
2.3. Starting the application	26
2.4. Home screen	27
2.5. Autodetecting a device	28
2.6. Searching for a device	30
2.6.1. TAC search	31
2.7. User predefined filter	33
2.8. Manual selection	35
2.9. Application toolbar	36

2.10. Case details	37
2.11. Investigation notes	38
2.11.1. Using the feature	39
2.12. Workflow guidance	45
<b>3. Advanced logical Android extraction</b>	<b>49</b>
3.1. The extracted data folder	55
<b>4. Settings</b>	<b>56</b>
4.1. General settings	57
4.1.1. Changing the application interface language	60
4.1.2. Changing the extraction location	64
4.2. Report settings	65
4.2.1. Managing report fields	67
4.3. System settings	69
4.4. License settings	70
4.4.1. License not found	71
4.4.2. Updating a dongle license online	74
4.4.3. Updating a software license online	76
4.5. Version details	79
4.5.1. Updates and versions	79
4.6. Commander settings	80
4.6.1. Connect a Cellebrite UFED device to Cellebrite Commander	82
4.6.2. Importing settings and configuration files	84
4.7. Activity Log	89

4.7.1. Exporting metadata to Cellebrite Commander .....	89
4.8. SOPs .....	90
4.8.1. Workflow guidance settings .....	91
4.9. Users permissions .....	92
4.9.1. Active Directory integration .....	93
4.9.2. Permission management .....	101
<b>5. Special cables .....</b>	<b>106</b>
5.1. Device power-up cable .....	106
5.2. Active extension cable .....	107
5.3. USB extension cable .....	107
5.4. USB cable for Cellebrite UFED Device Adapter V2 PowerUP .....	108
<b>6. Regulatory compliance .....</b>	<b>109</b>
<b>7. Specifications: Cellebrite UFED Device Adapter .....</b>	<b>110</b>
7.1. Specifications: Multi SIM Adapter .....	112
<b>8. Ordering cables and accessories .....</b>	<b>113</b>
<b>9. Glossary .....</b>	<b>116</b>
<b>10. Index .....</b>	<b>128</b>

# 1. Overview

Cellebrite UFED 4PC is a new generation solution that empowers law enforcement, military, intelligence, personnel to capture critical forensic evidence from Android and iOS mobile devices.

Cellebrite UFED 4PC enables you to:

- » Perform physical, file system, and logical extraction of device data and passwords. Capabilities may vary, based on the Cellebrite UFED 4PC product purchased - Cellebrite UFED 4PC Logical or Cellebrite UFED 4PC Ultimate.
- » Extract vital data such as call logs, phonebook entries, text messages (SMS), pictures, videos, audio files, ESN IMEI, ICCID and IMSI information and more, from a wide range of mobile devices.
- » Extract data from the widest selection of operating systems, such as Apple iOS, Blackberry, Android, Symbian, Microsoft Mobile, and Palm OS.
- » Clone the SIM ID, which allows you to extract phone data while preventing the mobile device from connecting to the network. It can also help if the SIM card is missing.
- » Extract the data from a mobile device either by a cable based connection (serial or USB) or a Bluetooth wireless connection. The tips and cable kit consists of four master cables and various tips.

The extracted data can be saved and then generated in the form of clear and concise reports.

Cellebrite's industry-expertise provides reliability and ease-of-use, and ensures the broadest support for mobile devices, including updates for newly released models before they are available to the market.



This manual is also relevant for Cellebrite Responder users.

## 1.1. System requirements

PC	Windows compatible PC with Intel i5 or compatible running at 1.9 GHz or higher	
Operating system	<p>Microsoft Windows 10, 64-bit Microsoft Windows 8.x, 64-bit Microsoft Windows 7, 64-bit Microsoft Windows 7 Boot Camp on MAC</p>	
Memory (RAM)	<b>Recommended</b> 16 GB	<b>Minimum</b> 4 GB
Space requirements	1.5 GB of free disk space for installation	
Additional requirements	Microsoft .Net version 4.5 or later	
Permissions	If you intend to activate the application using a hardware license key (dongle) provided by Cellebrite, you must have administrative rights over the computer.	



This specification is for a PC running both Cellebrite UFED 4PC and the Physical Analyzer application as the decoding operations of Physical Analyzer require the higher specification. For a standalone PC running Cellebrite UFED 4PC an ATOM based chipset (or equivalent) is sufficient.

## 1.2. Extraction types

Cellebrite UFED 4PC includes a range of data extraction types.



The available extractions may vary, based on the type of product purchased; the Cellebrite UFED 4PC Logical or the Cellebrite UFED 4PC Ultimate product.

Table 1-1: Functionalities of the Cellebrite UFED 4PC products

Functionality	Cellebrite UFED 4PC Logical	Cellebrite UFED 4PC Ultimate
Logical Extraction	Yes	Yes
SIM Data Extraction	Yes	Yes
Password Extraction	Yes	Yes
Clone SIM	Yes	Yes
File System Extraction	Not available	Yes
Physical Extraction	Not available	Yes
Capture Images/Screenshots	Optional	Yes
Chat capture	Yes	Yes

The extraction types are:

- » **Logical extraction:** Extracts user data from a mobile device (SMS, call logs, pictures, phonebook, videos, audio, certain application data, and more). Quickest extraction method but least amount of data.
- » **SIM card extraction:** Extracts data from a SIM or USIM card.
- » **File system extraction:** Extracts files embedded in the memory of a mobile device. Retrieve the artifacts within a Logical extraction, in addition to hidden system files, databases and other files which were not visible within a logical extraction.
- » **Password extractions:** Unlocks and displays passwords from a source mobile device.
- » **Clone SIM:** Copies a SIM ID from one SIM card to another SIM card or to a Cellebrite UFED SIM ID Access Card.
- » **Physical extraction:** Extracts a physical bit-for-bit image of the flash memory of a device, including the unallocated space using advanced methods. Unallocated space is the area of the flash memory that is no longer tracked by the file system, which may contain images, videos, files, and more.

- » **Capture images and screenshots:** Take pictures or videos of a device using the Cellebrite UFED camera. You can also capture internal screenshots directly from the connected device.
- » **Chat capture:** Chat Capture is an automated screen capturing process that allows users to extract and analyze selective chat conversations from third party application data.

### 1.3. Accessories

The Cellebrite UFED kit includes connection cables and tips. These are used in order to connect mobile devices to Cellebrite UFED.



Figure: Cellebrite UFED Cables and tips

The Cellebrite UFED Ultimate kit contains tips and cables for logical, file system, and physical extractions.

The Cellebrite UFED Logical kit contains tips and cables for Logical Extraction only.

### 1.3.1. Cellebrite UFED Device Adapter with USB 3.0

The Cellebrite UFED kit contains a device adapter that attaches to your PC's USB ports. Each connector has a LED that indicates availability during an extraction and blinks to indicate where to connect the source device. In addition, there are LEDs for power and Bluetooth.

Depending on when you received your kit, there are two types of device adapters: Cellebrite UFED Device Adapter with USB 3.0 (latest version) and Cellebrite UFED Device Adapter with USB 2.0 (previous version). This document provides more information on the Cellebrite UFED Device Adapter with USB 3.0.



This manual is also relevant for Cellebrite Responder users.



Some devices can be extracted only by using the Cellebrite UFED Device Adapter.



This device adapter has the following connectors:

- » GPIO port (for future use)
- » USB 3.0 port
- » RJ45 port
- » DC In power supply (Input 5.3V 3.7A)
- » 2 USB connection cables labeled POWER and DATA.

For information on the specifications, refer to the *Overview Guide*.

### To connect the Cellebrite UFED Device Adapter with USB 3.0:

1. First connect the DATA cable to a USB port on the computer.
2. Then connect the POWER cable to a second USB port on the computer.



Use the following procedure, if the computer is mounted in a difficult to access or distant location.

## To connect the Cellebrite UFED Device Adapter with USB 3.0 using extension cables:

1. Connect the **Active Extension cable**<sup>1</sup> to the DATA connection cable. Refer to the *Overview Guide*.
2. Connect the other end of this extension cable to a USB port on the PC.
3. Connect a standard USB extension cable to the POWER connection cable.
4. Connect the other end of this extension cable to a USB port on the PC.



### 1.3.1.0.1. Using the External power supply

The external power supply is NOT required for the smooth operation of the Cellebrite UFED Device Adapter V3, but is provided for those cases where additional power output is required. The external power supply provides an output of approximately 5.3V 2.7A.

### 1.3.2. Multi SIM Adapter

A Multi SIM Adapter supports Micro, Nano and standard SIM cards.



It is recommended to connect the Multi SIM Adapter to an available USB port on your computer, not to the USB port on the Cellebrite UFED Device Adapter.



---

<sup>1</sup>This cable is 150 cm in length and allows for the easy and accessible placement of the UFED Device Adapter with USB 3.0.

### 1.3.3. Using cables and tips

The cables and tips include various adapter cables (the number of cables depends on the Cellebrite UFED product and kit purchased). Each cable has a letter and name for example: A Adapter – USB.



*Figure: Single cable*

For easy recognition, the tips are color coded and numbered; the color represents the vendor.



*Figure: Cellebrite UFED tip (example)*

Before each extraction, the required cable and tip number and color is specified in the **Source** area of the Select Content Types screen.

## 1.4. Supported devices

To find out which mobile devices are supported in Cellebrite UFED and which data extraction capabilities are available for every mobile device use one of the following:

1. The Cellebrite UFED <version no> Supported Phone List file is delivered with every Cellebrite UFED software version update. The Microsoft Excel file contains two worksheets:

The **Cellebrite UFED Logical** sheet lists the mobile devices supported for logical extraction.

The **Cellebrite UFED Physical** sheet lists the mobile devices supported for physical, file system, and password extractions.

2. **UFED Phone Detective** (devices supported for logical extraction only).
3. Cellebrite UFED Supported Devices document in [MyCellebrite](#).

## 1.5. Cellebrite YouTube channel

For your convenience, a selection of useful videos demonstrating typical workflows and common procedures are available at [youtube.com/cellebriteufed](https://youtube.com/cellebriteufed).

## 2. Getting started

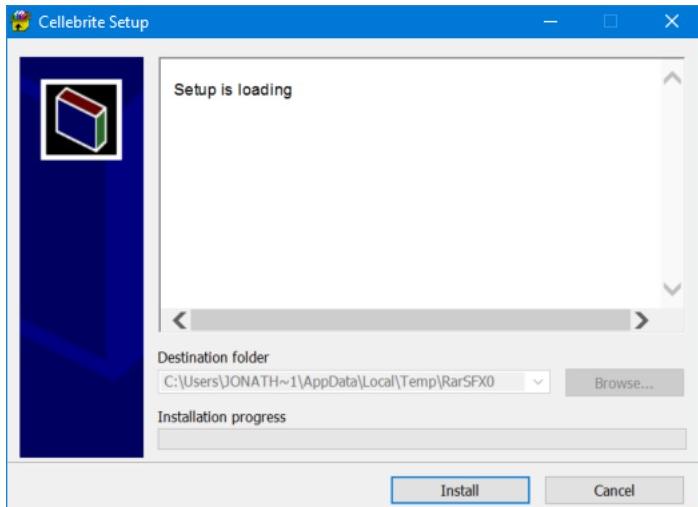
This section includes the following:

2.1. Installing Cellebrite UFED .....	17
2.2. Activating the license .....	21
2.3. Starting the application .....	26
2.4. Home screen .....	27
2.5. Autodetecting a device .....	28
2.6. Searching for a device .....	30
2.7. User predefined filter .....	33
2.8. Manual selection .....	35
2.9. Application taskbar .....	36
2.10. Case details .....	37
2.11. Investigation notes .....	38
2.12. Workflow guidance .....	45

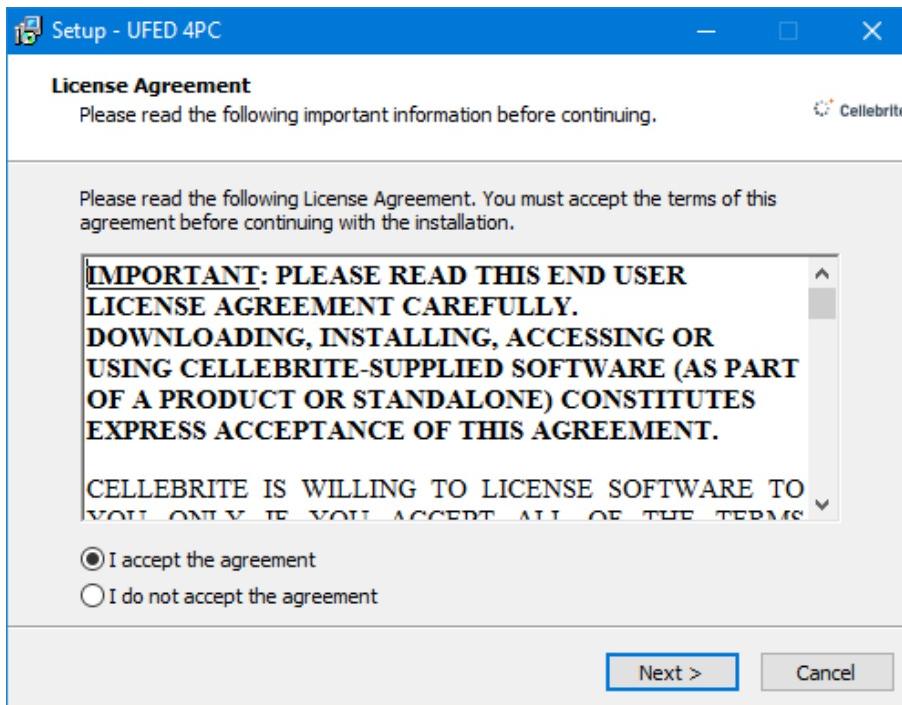
## 2.1. Installing Cellebrite UFED

To install Cellebrite UFED:

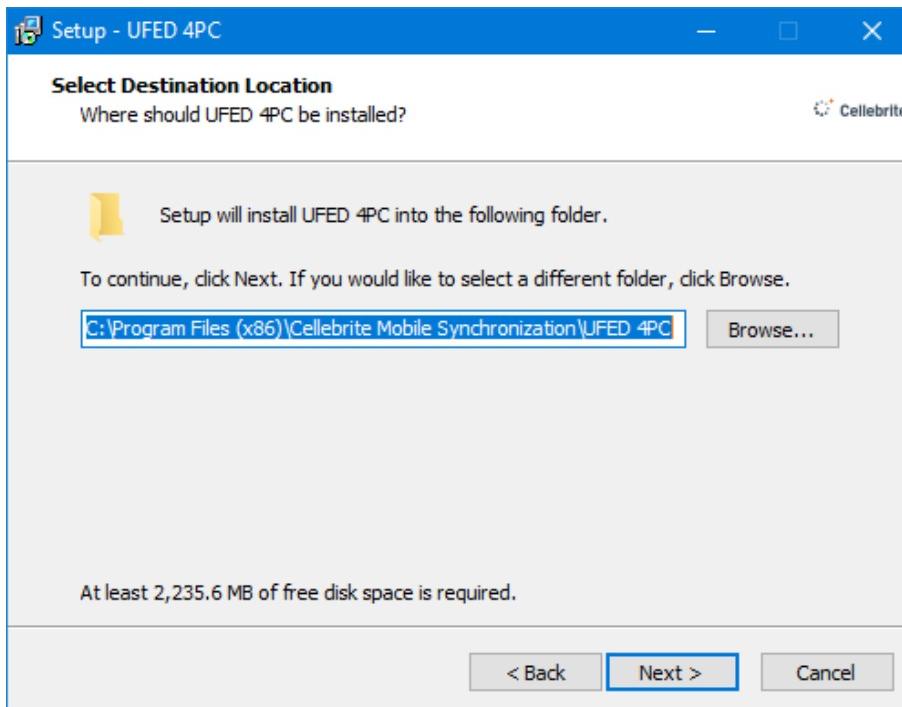
1. Start the Cellebrite UFED installation wizard. The following window appears.



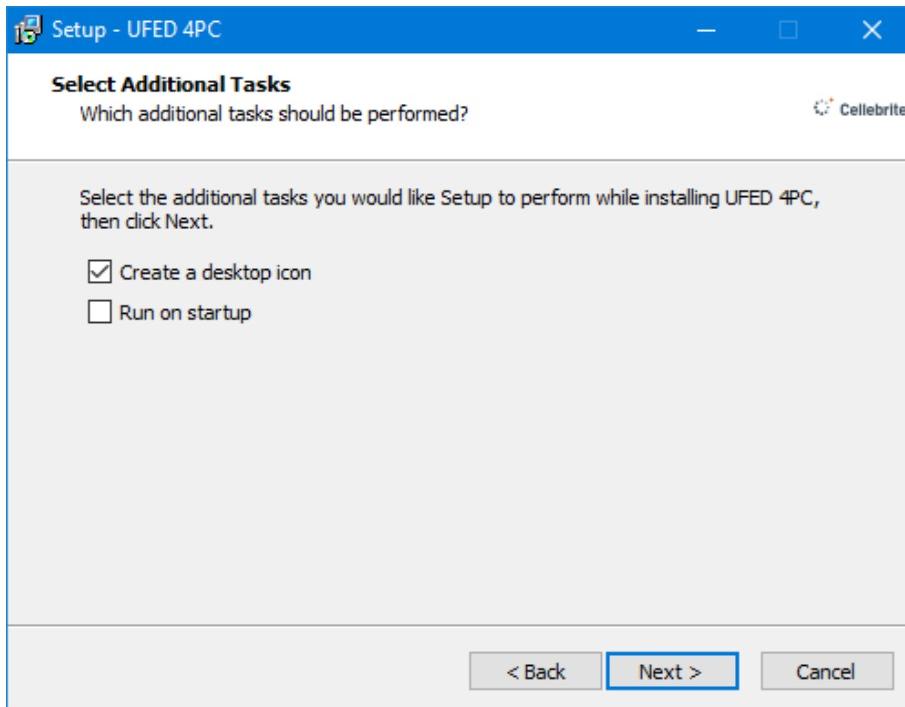
2. Click **Install**. The License Agreement window appears.



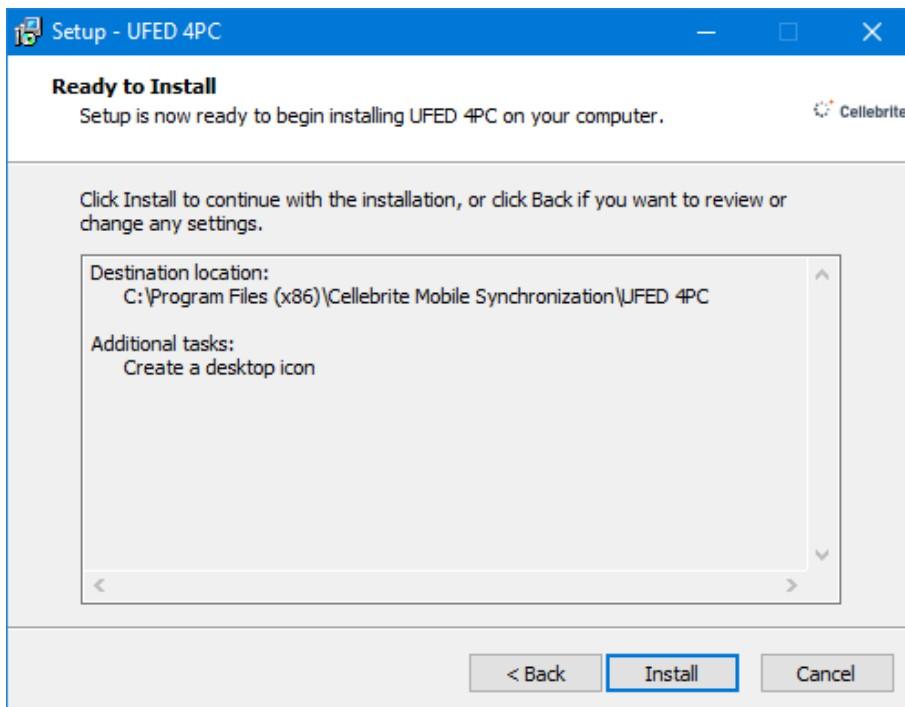
3. Select **I accept the agreement**, and click **Next**. The Select Destination Location window appears.



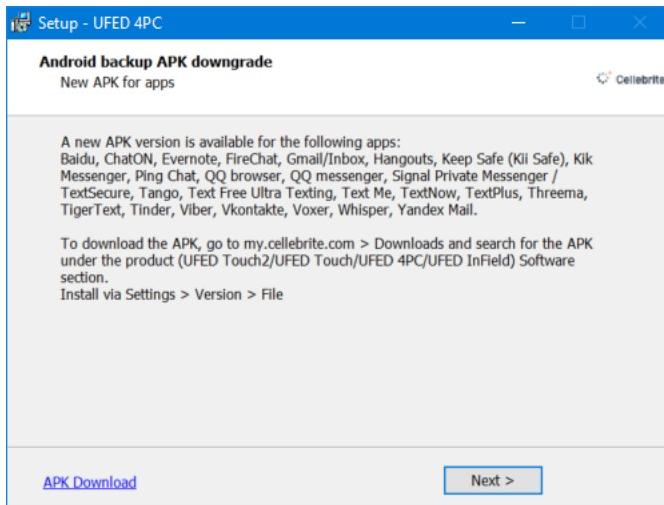
4. Select the folder where you want the application installed, and click **Next** to continue. The Select Additional Tasks window appears.



5. Select the additional tasks you want the install wizard to perform, and then click **Next**. The Ready to Install window appears.



6. Click **Install**. The following window appears.

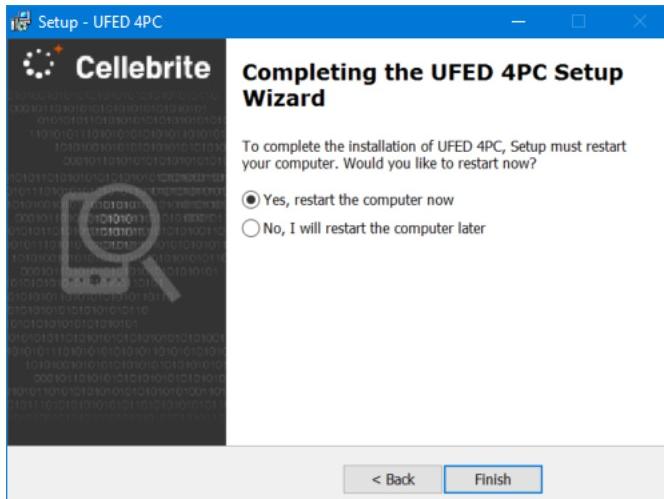


7. Click the **APK Download** link to go to [MyCellebrite](#) and search for and download the new APK under the Cellebrite UFED Software section. The new APK will enable Android backup APK downgrade support for additional app versions.



Install the APK via **Settings > Version > File** after completing the Cellebrite UFED installation process.

8. Click Next. The following window appears.



9. Select **Yes, restart the computer now**, and click **Finish** to restart the computer.

You must now activate the license to use Cellebrite UFED. Proceed to [Activating the license \(on the next page\)](#).

## 2.2. Activating the license

Activate Cellebrite UFED in one of the following ways:

- » [Using a dongle license \(below\)](#)
- » [Using a network dongle \(on page 25\)](#)



Check your Cellebrite UFED kit to make sure which method you should use.



If you are using Cellebrite UFED for the first time or a license is not found, see [License not found \(on page 71\)](#).

### 2.2.1. Using a dongle license

Use the Cellebrite UFED dongle provided with your Cellebrite UFED kit. The dongle contains licenses for all the applications purchased.



**To use Cellebrite UFED with a dongle:**

1. Go to [community.cellebrite.com](#) and log in with your credentials (or create an account).
2. Go to **Products & Licenses > Register Device** and enter a name for the device, the serial number and Dongle ID as displayed on the dongle.

### Register New Device

\* Device name

\* Serial number

\* UFED/Dongle ID

[Next](#)

3. Click **Next**. The following window appears.

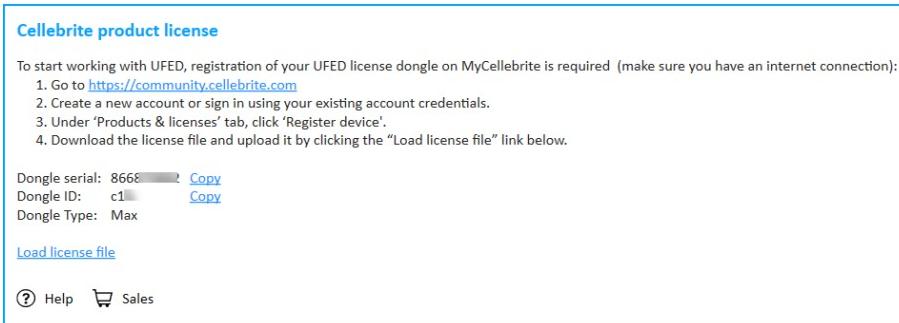
### Device Registration completed

Download license for device Serial number: to activate your product

[Download License](#)

[Done](#) [Register Another Device](#)

4. Click **Download License** from the Device Registration Completed window to download the license key (or click **See licenses** in the Products tab and then from the menu on the right select **Download license**).
5. Download and install the Cellebrite UFED application.
6. Start the Cellebrite UFED application and connect the dongle to a USB port on your computer. The following window appears.

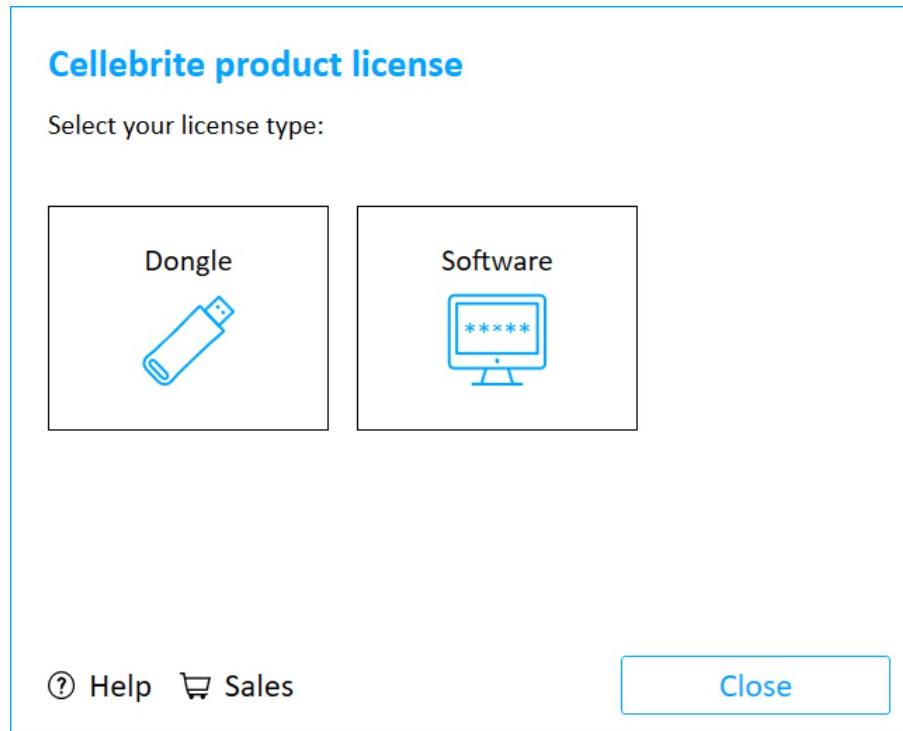


7. In the Cellebrite product license window, click **Load license file** and upload the license key.

Congratulations, your Cellebrite UFED application is now ready!

If a license dongle is not found:

- When a license dongle is not found, the Cellebrite product license window appears.



- Click **Dongle**. If you connected the dongle to a USB port on your computer, and it still does not work, contact [support@cellebrite.com](mailto:support@cellebrite.com).

## 2.2.2. Using a network dongle

The network dongle is connected to your organization's network and contains licenses for all the applications purchased.

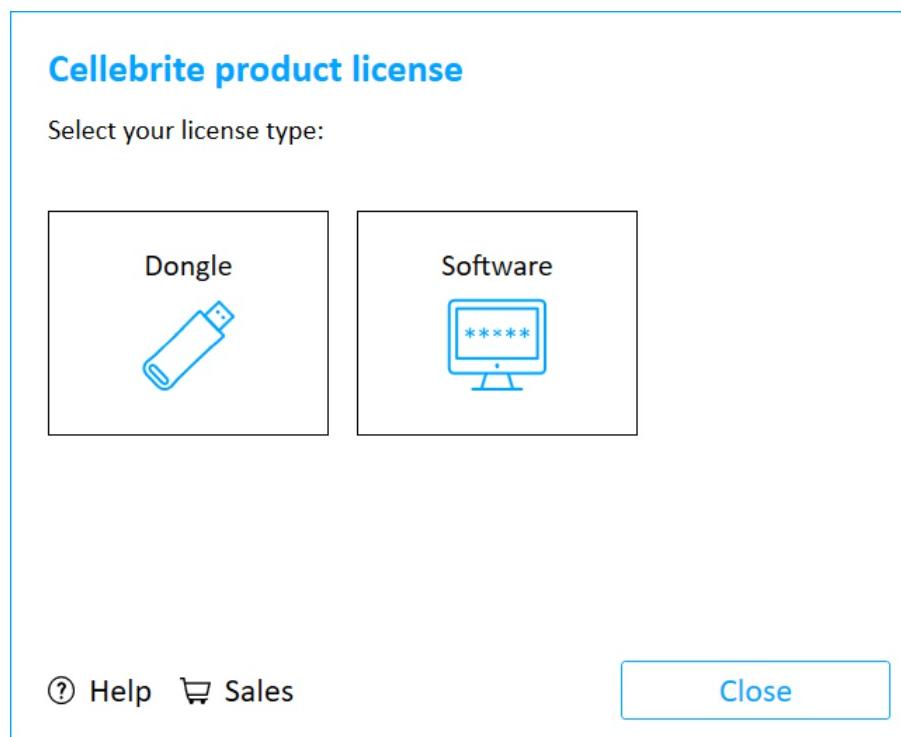


**To use Cellebrite UFED with a network dongle:**

- » Start the application. If the network dongle is connected to the network, the application starts and you can start working immediately.

**If a network dongle is not found:**

1. If the network dongle is not recognized, the Cellebrite product licensing window appears.



2. Click **Network**. The following window appears.



If a dongle was not found on the network. Make sure that you have an Internet connection and that a dongle is connected to the network. Then click **Refresh** to search for a network dongle again.



If you click **Refresh** twice, a new window will appear where you can manually connect to the network dongle. Click **Advanced** and then enter the IP address (or host name).



If there is only one network dongle it will be selected automatically. If there are multiple network dongles, select the required Dongle Serial number.

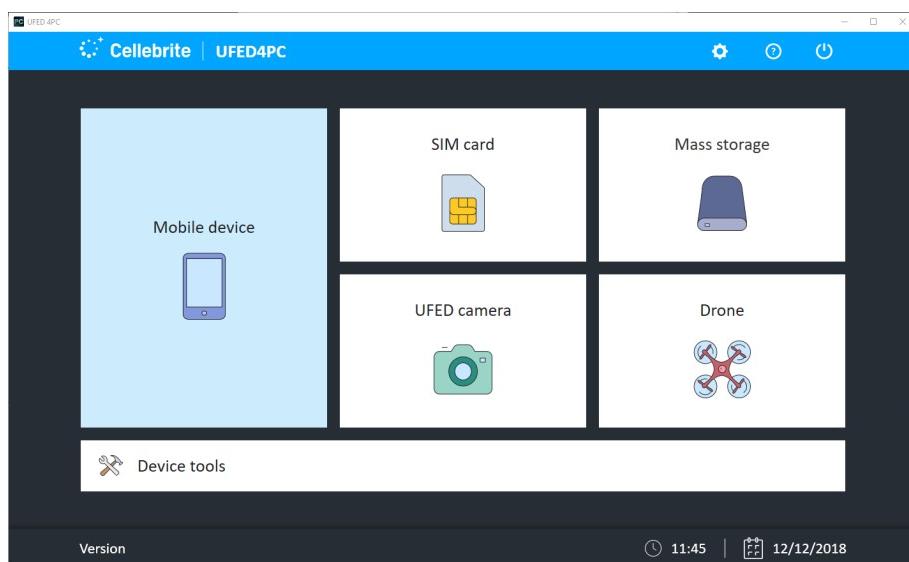
Congratulations, your Cellebrite UFED application is now ready!

### 2.3. Starting the application

- » Double-click the Cellebrite UFED icon to open the application.

## 2.4. Home screen

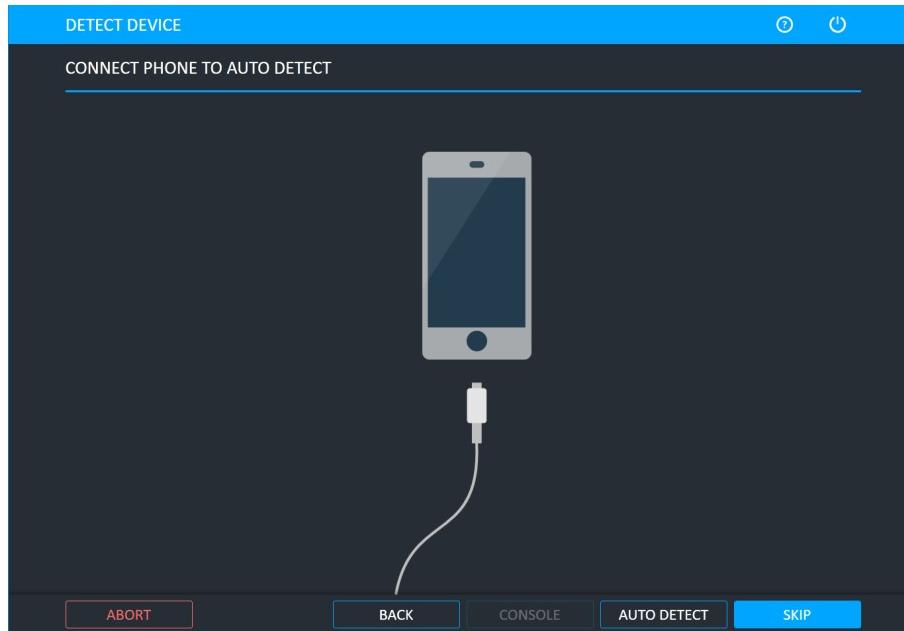
The home screen groups the extraction data into distinct areas: Mobile device, SIM card and USB device or Memory card. In addition, users can directly operate the camera for immediate image capturing or access the device tools. All extraction functionality is driven by **automatic** identification of the device, by **searching** for the device or by **manually** selecting the vendor and model. Cellebrite UFED determines what functions are available for the specific device and displays the relevant functions.



## 2.5. Autodetecting a device

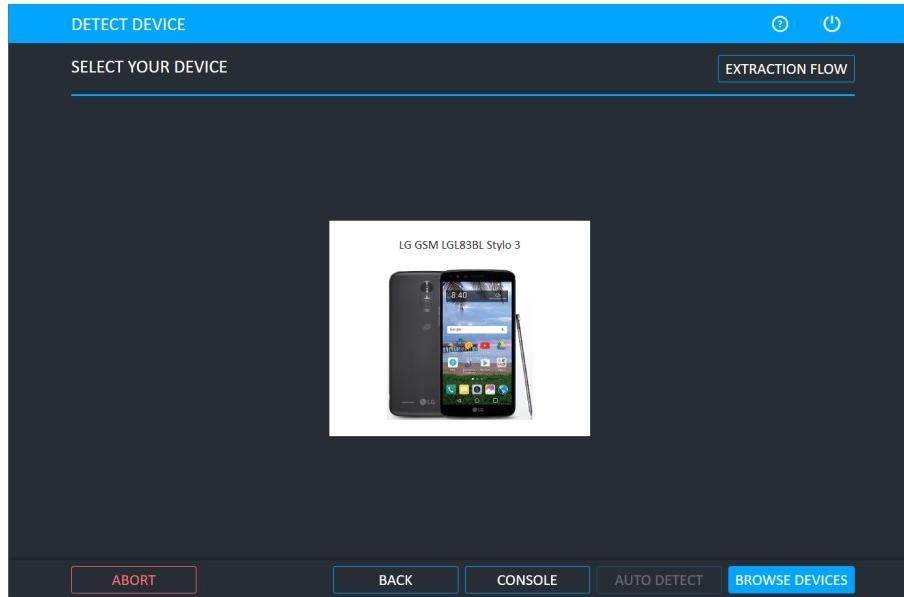
To use Autodetect to locate the mobile device:

1. Connect the mobile device to the Cellebrite UFED unit.

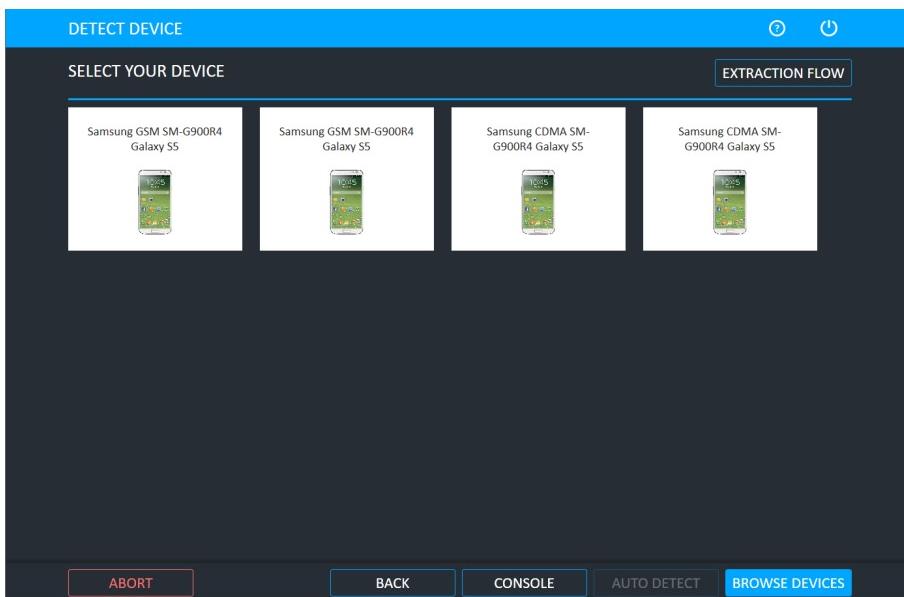


2. Select **Auto Detect** at the bottom of the screen.

If the connected device is recognized by the system the following window appears.



If multiple matches are found, the following window appears.

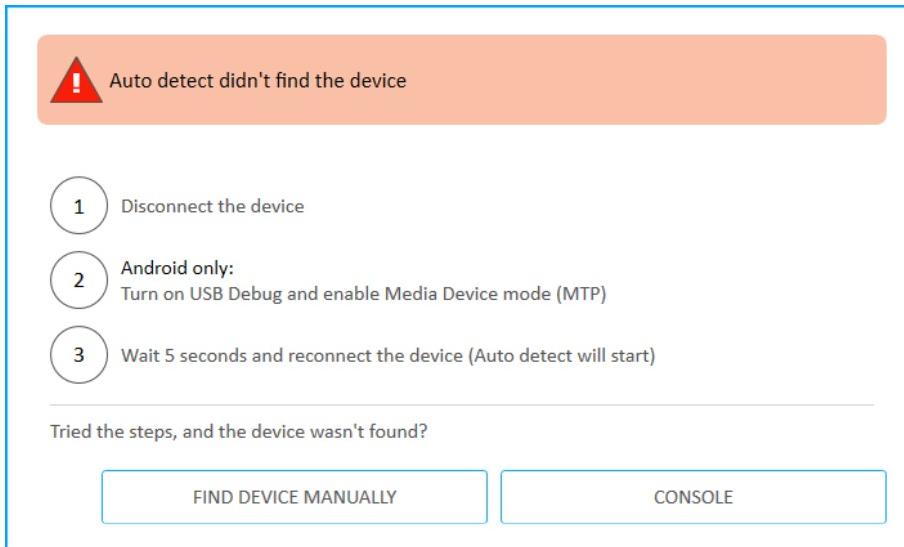


3. Select the relevant device.
4. Alternatively, click **Browse Devices** to manually search for the device.



Click the **Console** button to access device information using the Android Debug Console. For more information, refer to the *Performing extractions* manual.

5. If the connected device cannot be recognized by the system, a message prompts you to try the following steps or tap Find device manually.

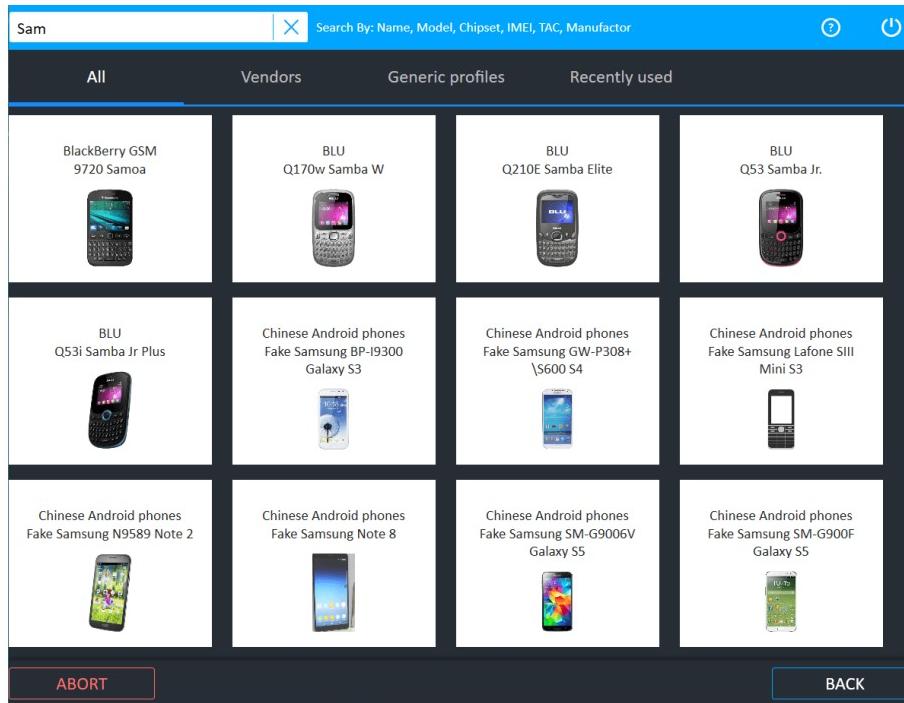


6. If the device still cannot be found, tap **Browse Devices** or **Console**.

## 2.6. Searching for a device

To search for the mobile device:

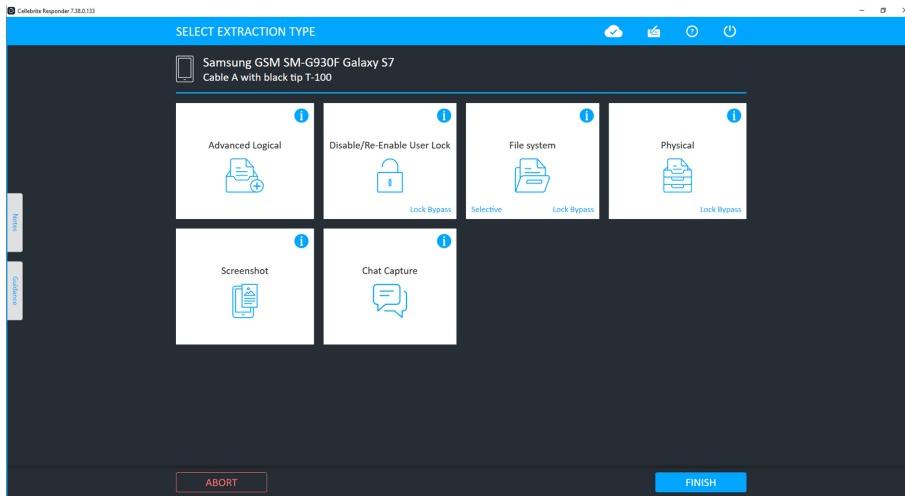
1. Narrow the list by vendor, recently used, etc. or begin typing in the search box in the top bar to search for a device or model. As you type, the list of devices is reduced to match your search criteria.



You can also search for a device by its IMEI value, which is used to uniquely identify devices. The IMEI value is usually found printed inside the battery compartment of the device, or dial \*#06# from the phone keypad. Enter the value in the search box, using a minimum of four digits up to the full number. If the IMEI value is recognized, matching devices will be displayed.

2. Select the device model type from the list.

Having selected the **device**, Cellebrite UFED will determine what extraction functions are available for this combination and present those functions as follows:



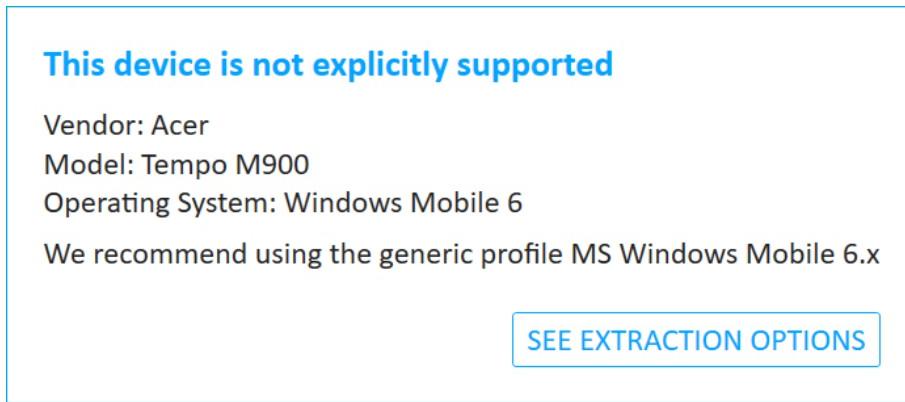
Lock Bypass is displayed for both physical and file system extraction methods that can bypass the user lock of the device.

### 2.6.1. TAC search

If you cannot find the Android device which you are looking for after performing a TAC number search, a window will appear. This window appears if Cellebrite UFED does not support the device directly, but there are applicable generic options available for the device.

**To retrieve device information and view generic extraction options:**

1. Enter the complete 8-digit TAC number. The following window appears.

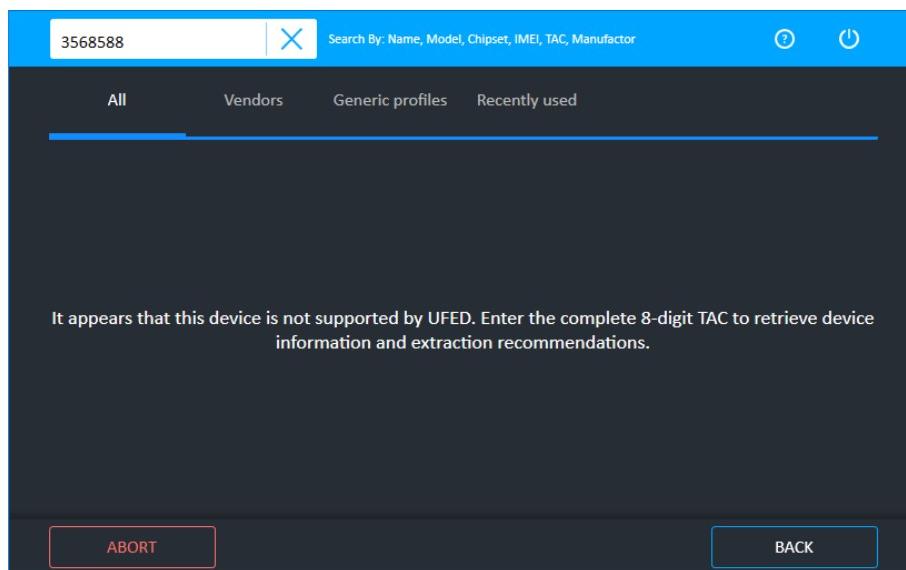


The window includes the vendor, operating system and device name.

2. Click **See recommended extractions**. A window appears with the generic extraction options for the device. An example appears next.



If you enter a partial TAC number (with less than 8-digits) or the device is not supported by Cellebrite UFED then the following window appears.



## 2.7. User predefined filter

The User predefined filter provides the ability to extract and view only a portion of the device content, based on time range or specific subject information (person, email, phone). This can be useful when:

- » The agency has a warrant to extract data from a specific time window, and is not allowed to view additional data that is not covered by the warrant.
- » The user wishes to save time and get to the relevant data ASAP.

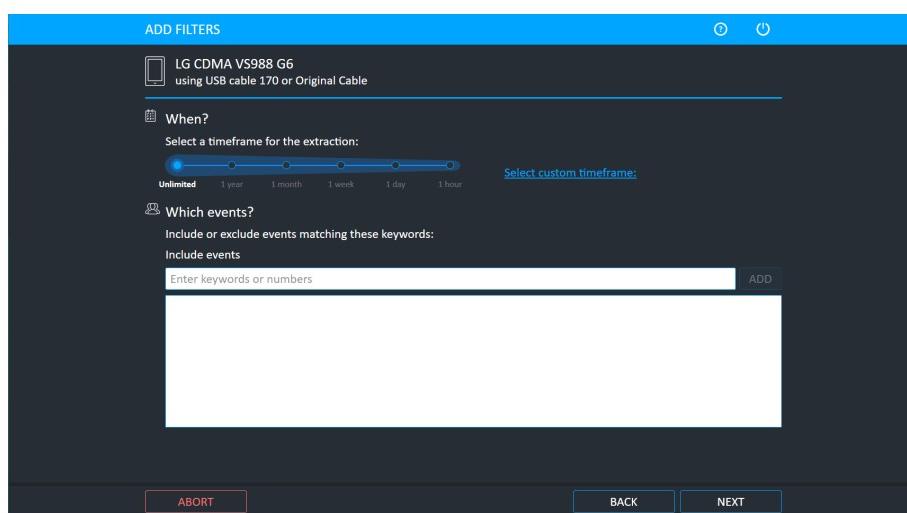
The most time consuming phase during a device extraction is transferring the data from the mobile device to the extraction tool. Timeframe filtering is performed on the device (when technically supported), and can reduce the extraction time. Another advantage is the reduced amount of data that the agent needs to browse through in order to find the evidence.

### To enable the User predefined filter:

- » Select **Allow user predefined filter** under **Settings > General**. For more information, see [General settings \(on page 57\)](#).

### To specify the timeframe and parties for the extraction:

1. Identify the device and select an extraction type. The following window appears.



The extraction is based on the Cellebrite UFED unit's date and time. When selecting a time frame you should also consider the device's time zone.



The timeframe option is not applicable to file system extractions.

2. Select the required time frame. The less time selected, the quicker the extraction.
3. Enter keywords or numbers that you would like to include.



Selective extraction by party: Similar to the time frame, the ability to extract and review only data relevant to a specific party (number or device).



Partial numbers will be matched by the application, and names are matched irrespective to the capitalization.

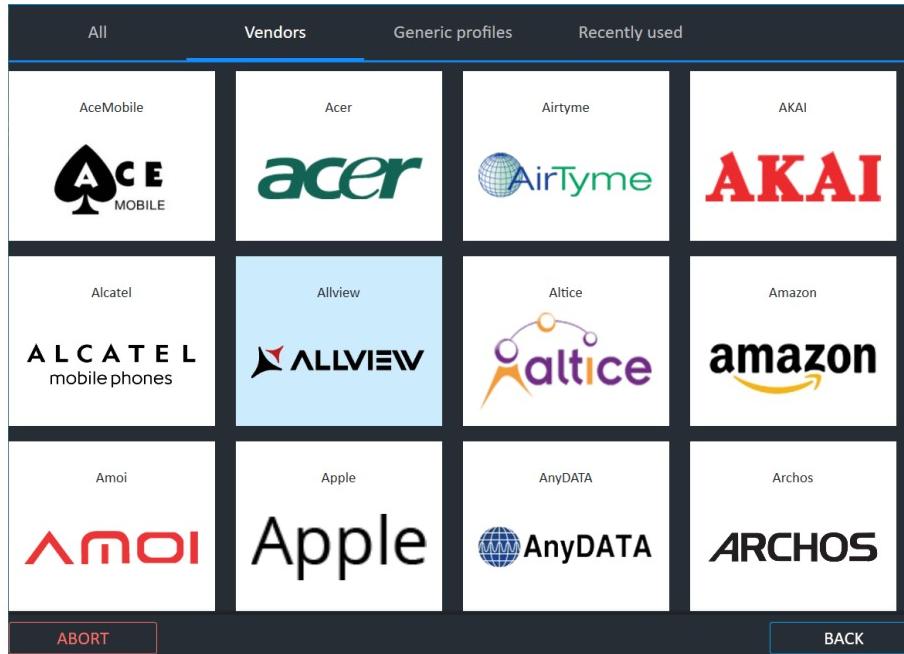
4. Click **Next**.

## 2.8. Manual selection

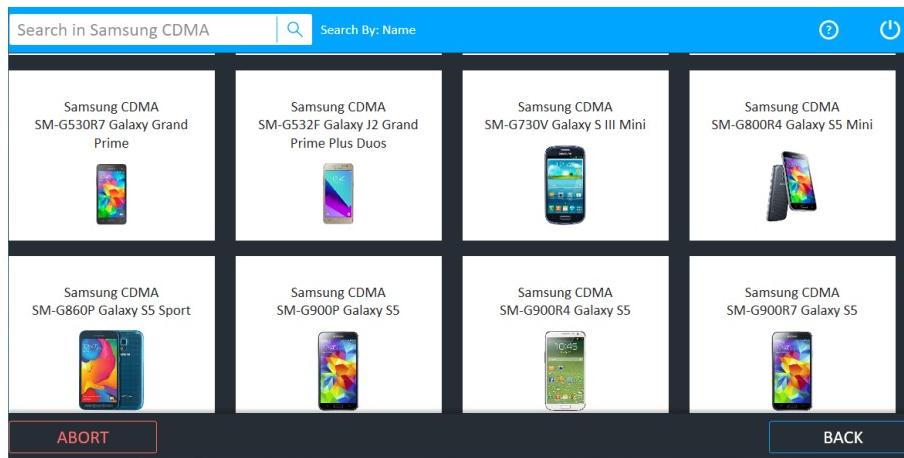
To manually select the vendor and model:

1. Click **Mobile device** and then click **Skip**.

You can then select **All**, **Vendor**, **Generic profiles**, or **Recently used**. As displayed next, the Vendor screen enables you to select the device vendor.



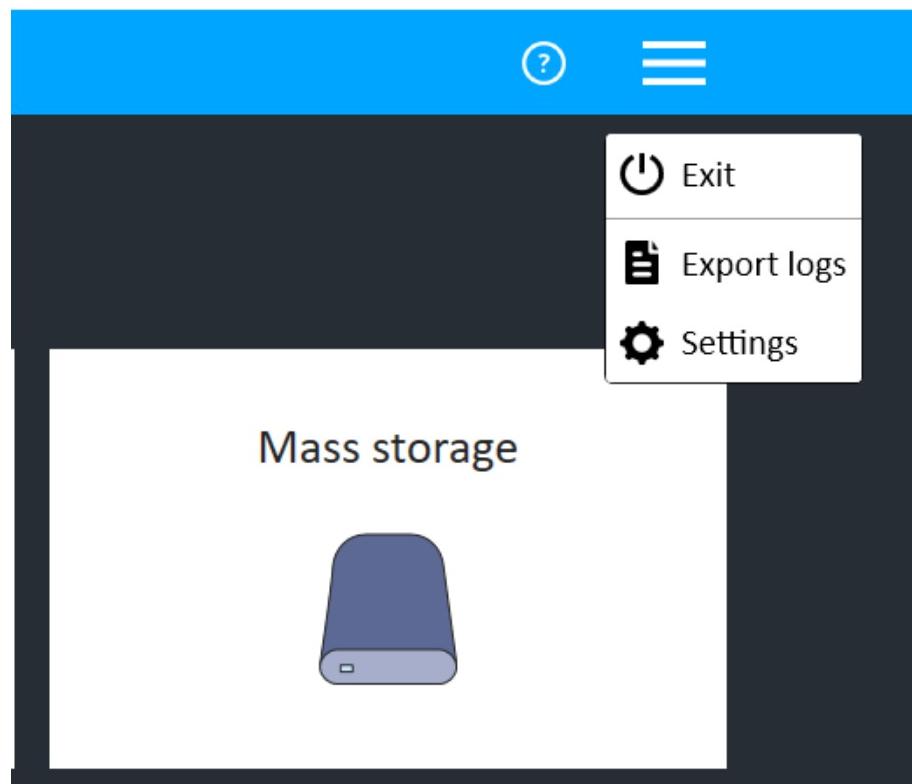
2. After choosing the Vendor, the application presents the Select Model screen where the specific model of the device is chosen:



Having chosen the **Vendor** and the **Model**, Cellebrite UFED will determine what extraction functions are available for this combination and present those functions.

## 2.9. Application toolbar

The application toolbar is located at the top of the screen.



Application toolbar icons and descriptions

Icon	Description
	Click to select Online help or Extraction flows document.
	Click the menu icon to access the following: <ul style="list-style-type: none"><li>»  Exit</li><li>»  Export logs</li><li>»  Settings</li></ul>

## 2.10. Case details

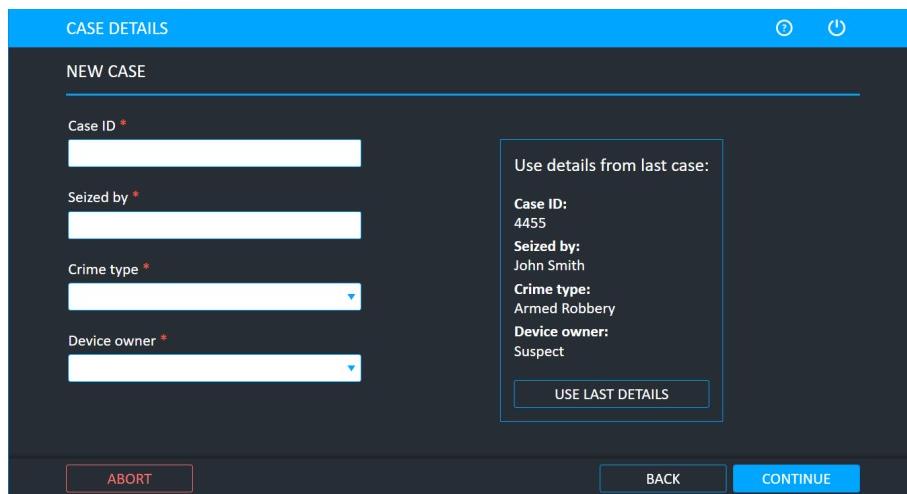
The Case details feature enables you to enter case details when performing an extraction or using the Cellebrite UFED camera. This feature is not enabled by default.

### To enable the case details feature:

- » Select **Include Case details screen** under **Settings > General**. For more information, see [General settings \(on page 57\)](#).

### To specify the case details:

1. On the Home screen, select an extraction type or Cellebrite UFED camera. The following window appears.



2. Use the current case information, or enter and select the case information and then click **Continue**.



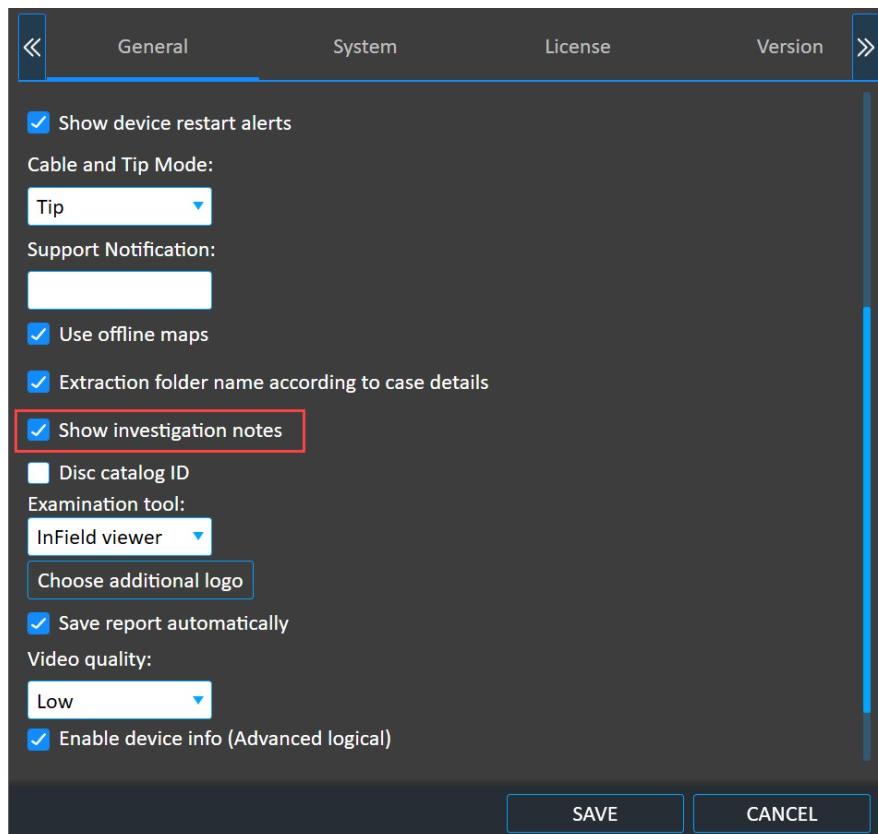
The Crime Types list can be changed via the Cellebrite UFED Permission Manager ([Using the Cellebrite UFED Permission Manager \(on page 101\)](#)) or Cellebrite Commander (refer to the Cellebrite Commander manual).

## 2.11. Investigation notes

The Investigation notes feature enables you to add notes during the data extraction process. You can include observations or report any issues encountered during the process.

To enable or disable the feature:

1. Select **Settings > General**. The following window appears.

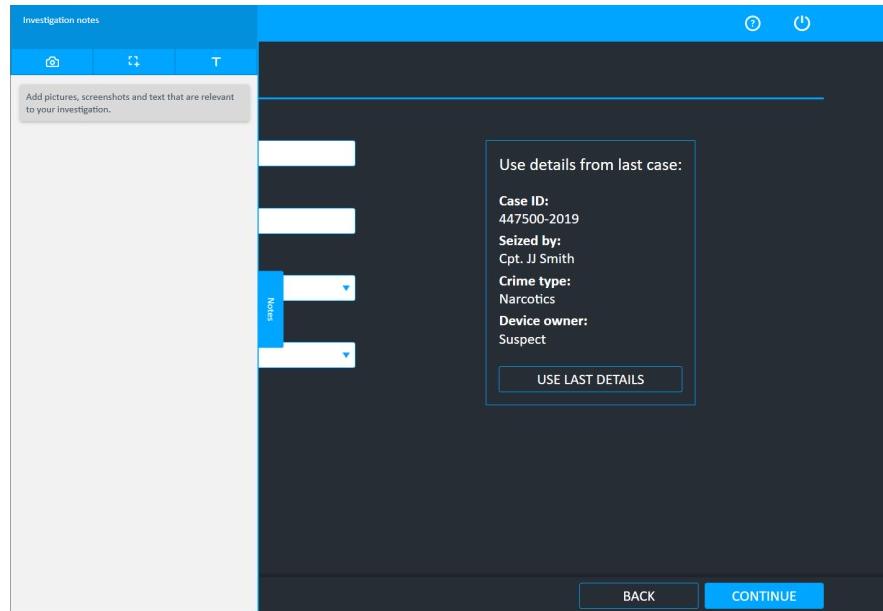


2. Select or clear the **Show investigation notes** check box.
3. Click **Save**.

## 2.11.1. Using the feature

You can add pictures, screenshots and text that are relevant to your investigation to create an audit trail of actions taken and decisions made.

1. Start an extraction and click **Notes**. The Investigation notes window appears.



To close the window, click the Cellebrite UFED interface outside of the Investigation notes window.

2. Add text, screenshots and pictures that are relevant to your investigation. The investigation notes are available as part of the extracted data or report. See [Investigation notes \(on the previous page\)](#)

See the following procedures to add text, screenshots and pictures:

[To add text notes: \(on the facing page\)](#)

[To add screenshots: \(on page 41\)](#)

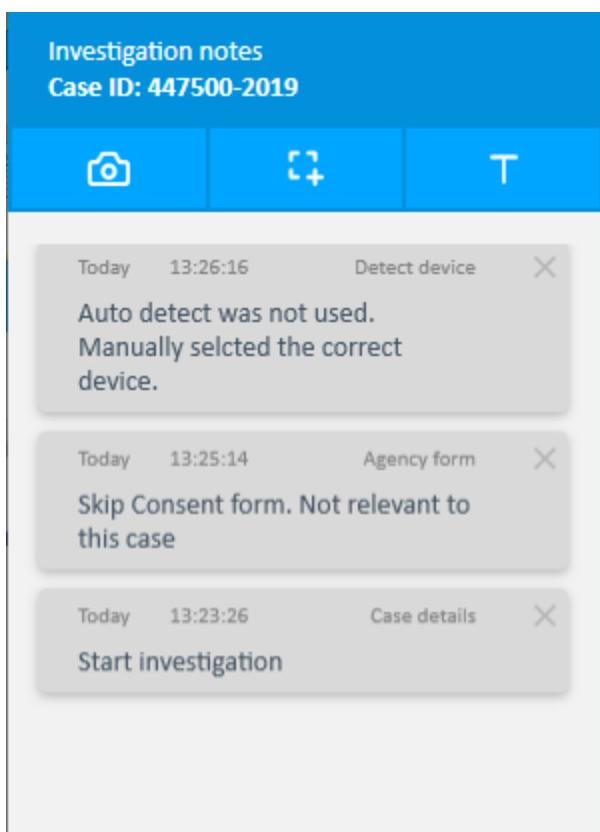
[To add pictures: \(on page 42\)](#)

## To add text notes:

1. In the Investigation notes window click Text (**T**). The following window appears.



2. Enter the required text and tap **Save**.
3. The text is added to the Investigation notes panel and it includes the date, time and stage of the extraction process. An example is displayed next.

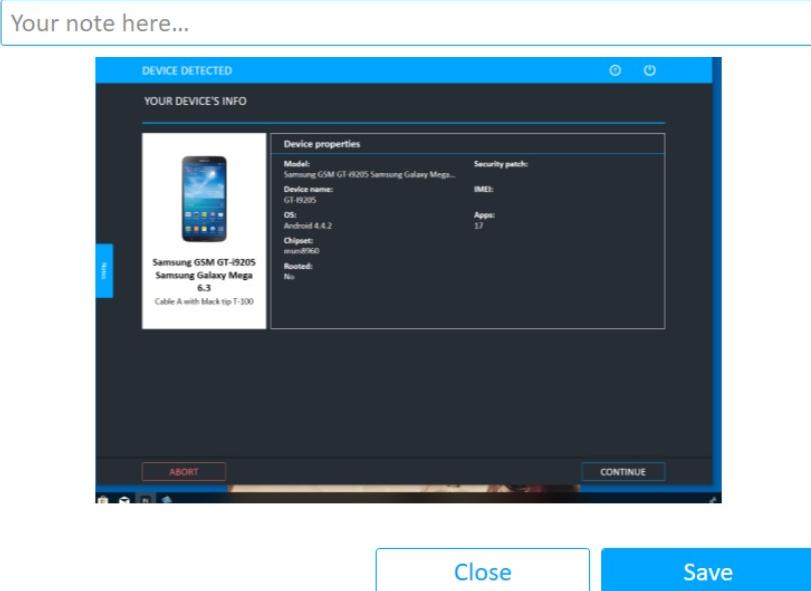


To remove a note click Delete (X).

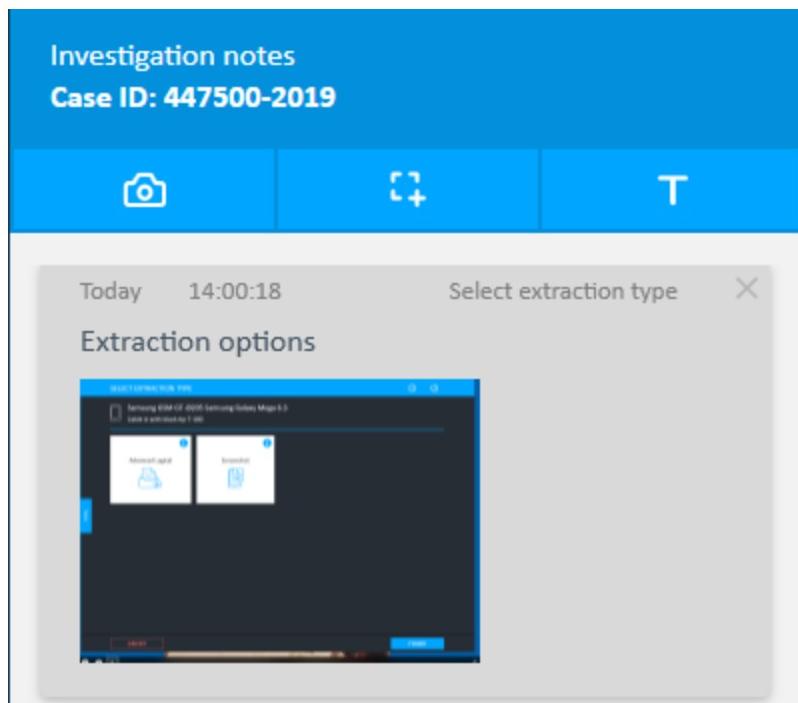
## To add screenshots:

1. In the Investigation notes window click Screenshot (). The following window appears.

### Insert text



2. Enter the required text and tap **Save**.
3. The screencapture is added to the Investigation notes panel and it includes the date, time and stage of the extraction process. An example is displayed next.



## To add pictures:

1. In the Investigation notes window click Picture (📷). The following window appears if a camera is not connected.

### Insert text

Your note here...



Camera not connected

Close

Save

2. Connect a camera to Cellebrite UFED.

### Insert text

Your note here...

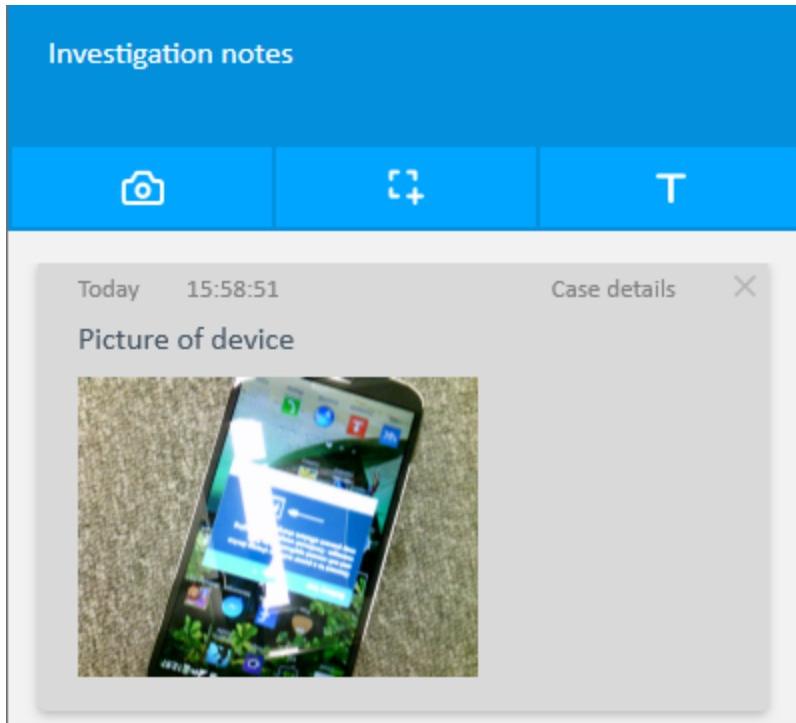


IPEVO Point 2 View ▾

Close

Save

3. Select the required camera to use.
4. Click Camera (  ) to take a picture. If required, tap Refresh (  ) to take a new picture, or click Rotate (  ) to rotate the picture.
5. Enter the required text and tap **Save**.
6. The picture is added to the Investigation notes panel and it includes the date, time and stage of the extraction process. An example is displayed next.



### 2.11.1.1. Accessing the extraction notes file

After completing the extraction, the investigation notes will be displayed as an ExtractionNotes.pdf file in the Notes folder when the report or extraction is saved.



In Cellebrite UFED, the PDF file is only created when you click **Finish**.

Examples are displayed next.

**Notes**

Share View

📁 <> Case ID 447500-2019 (001) (5) > Notes > ⏺ 🔍 Search

Name	Date modified
📁 Images	2/20/2020 12:19 PM
📝 ExtractionNotes.pdf	2/20/2020 12:19 PM
📝 ExtractionNotes.xml	2/20/2020 12:19 PM

*Folder location*

### UFED investigation notes

Cellebrite  
www.cellebrite.com

**Summary**  
**Notes (4)**

1/4

Time stamp	2/23/2020 4:26:14 PM (GMT+2)
Application state	Detect device
Camera note	 <a href="#">Click to enlarge</a>

2/4

Time stamp	2/23/2020 4:26:23 PM (GMT+2)
Application state	Detect device
Screenshot note	 <a href="#">Click to enlarge</a>

*Example Investigation notes*

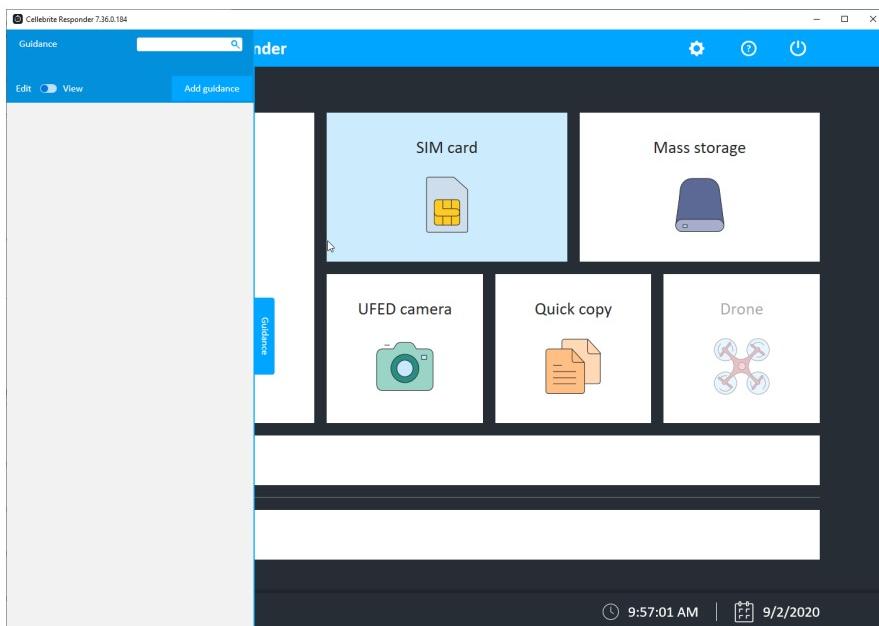
## 2.12. Workflow guidance

Workflow guidance allows admins to create guided instructions to assist users during the workflow. Workflow guidance can be made mandatory to ensure users read the guidance. To manage Workflow guidance, see [Workflow guidance settings \(on page 91\)](#).

### Creating Workflow guidance

1. From the main screen, click the **Guidance** tab.

The Guidance panel appears.



2. Click the toggle button to enable **Edit** mode.
3. Click **Add guidance**.

The Edit guidance window appears.

## Edit guidance

### Guidance title

Insert title here...

### Guidance text

Insert guidance text here...



Image



Show guidance message on first login only.

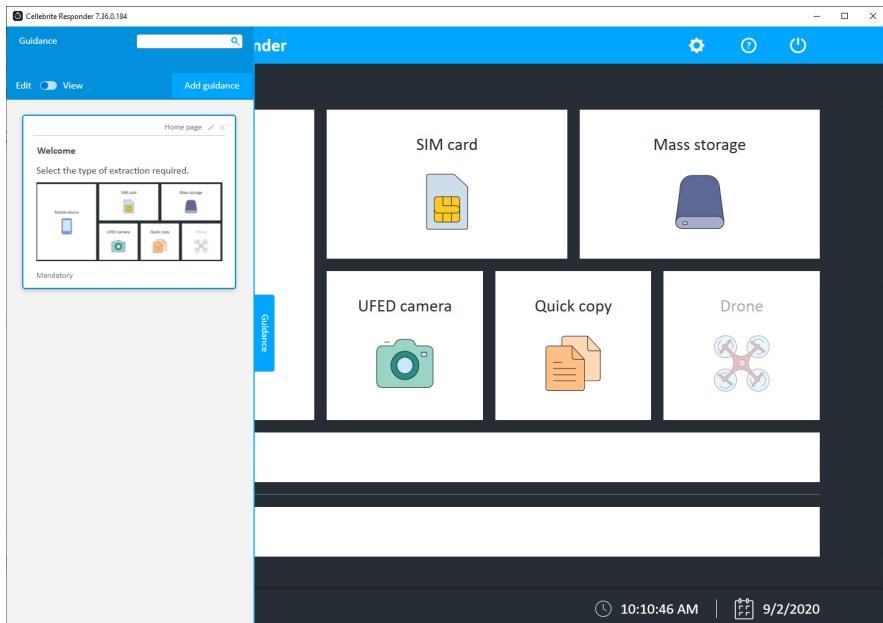
Make guidance mandatory

Cancel

Save

4. Enter the guidance title and text.
5. Add an image (optional).
6. Select **Show guidance message on first login only** (optional).
7. Select **make guidance mandatory** (optional).
8. Click **Save**.

The new guidance will appear in the Guidance panel.



9. Continue adding the required guidance for each screen in the workflow. The guidance will appear on the screen from which it was created.

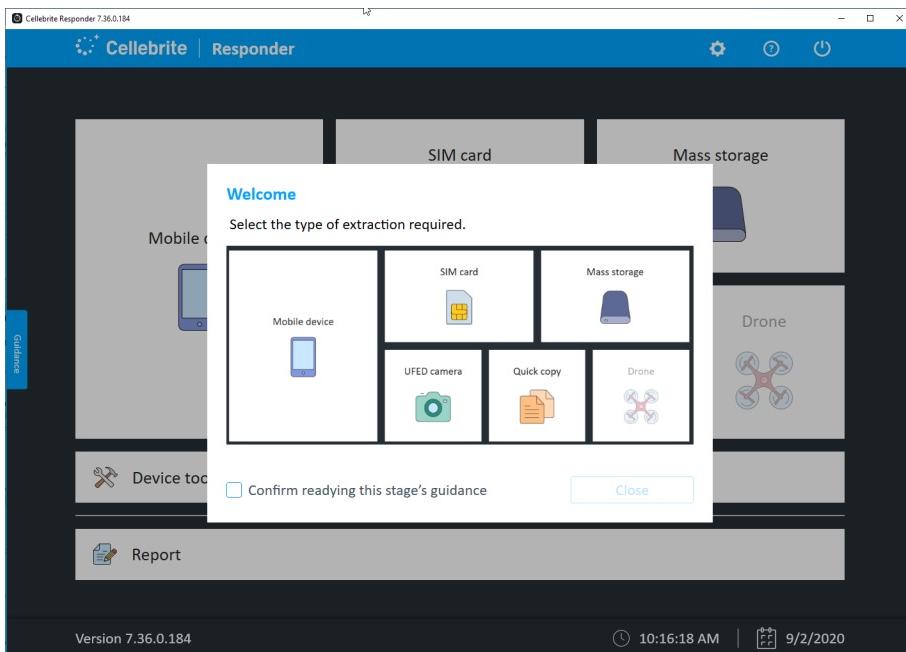


There can only be one guidance added to each screen.

## Using Workflow guidance

The Workflow guidance added by the admin will appear during the workflow stages.

In the example below, the home screen guidance appears when opening Cellebrite UFED 4PC.



1. Review the guidance.
2. Check **Confirm reading this stage's guidance**.



This will be displayed if the guidance was made mandatory by the admin in the Workflow guidance settings.

3. Click Close.

### 3. Advanced logical Android extraction

The following procedure explains the Advanced logical extraction process for an example device. The procedure may vary depending on the selected device. This section shows only one of the many extraction types that can be performed.

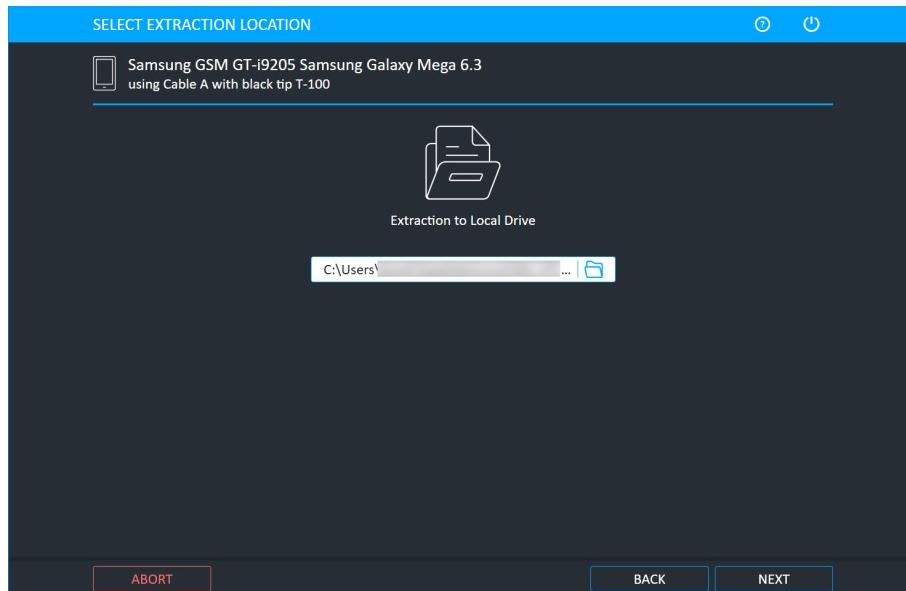
#### To perform an Advanced logical extraction from a mobile device:

1. Click **Mobile device** and identify the device, then click **Advanced Logical**.

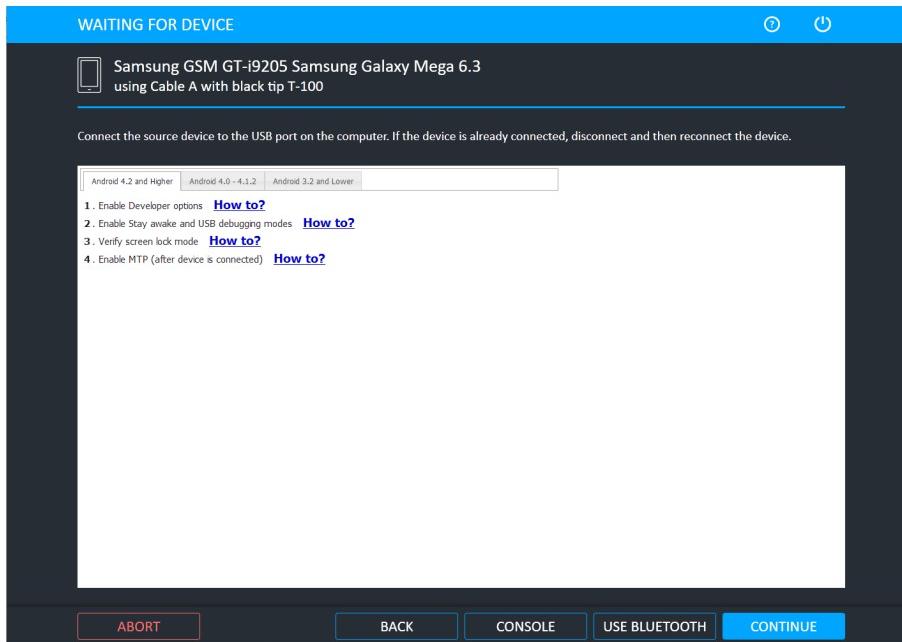


For information on using optional timeframe and party filters, refer to the *Overview Guide*.

The Select Extraction Location window appears.

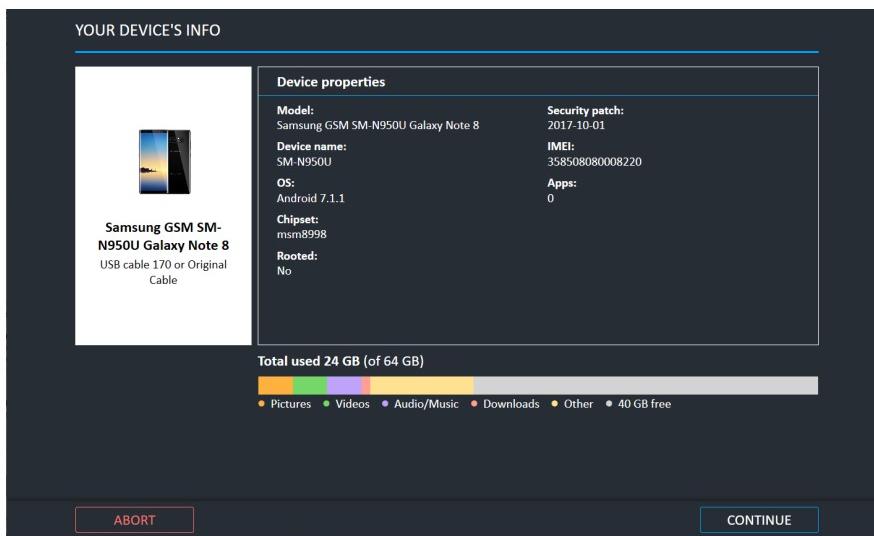


2. Use the current location or click the folder icon to change the target path and select a different location and then click **Next**. The Waiting for Device window appears.



Click the **Console** button to access device information using the Android Debug Console. For more information, refer to the *Performing extractions* manual.

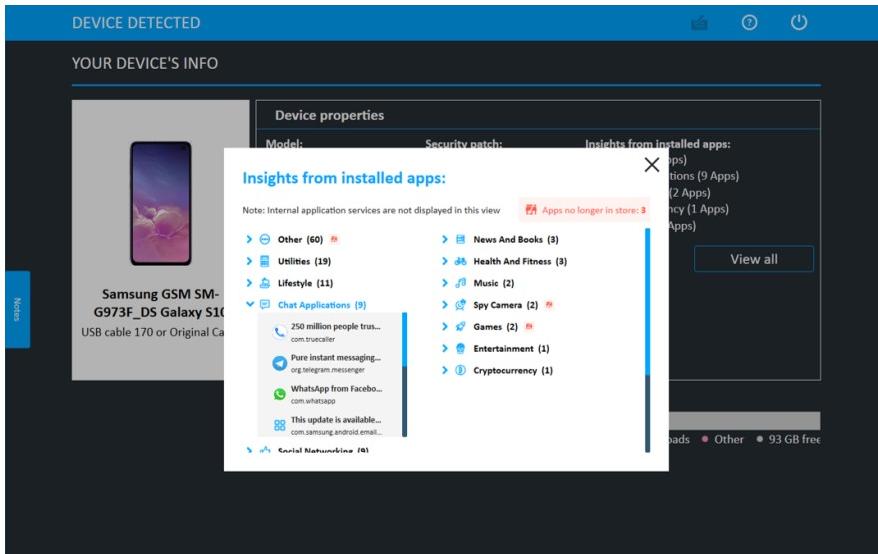
3. Select the correct cable and tip for the mobile device, and change the device settings according to the instructions.
4. Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.
5. Click **Continue**. The following window appears if the Enable device preview info screen option is enabled under General settings.



This window provides information on the device data before performing an Android extraction. It includes device properties such as model, device name, OS, chipset, whether the device is rooted, date security patch installed, IMEA, the number of installed apps, and insights from installed apps.

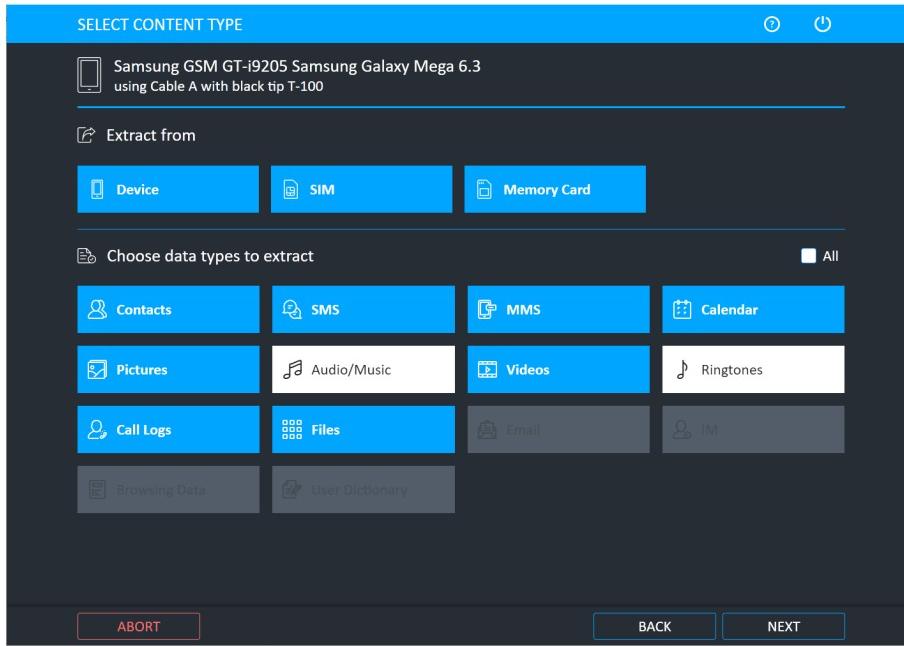
Insights from installed apps allows the user to get a peek into the types of apps installed on the device before the extraction. This area displays app categories and the number of apps in each. Click **View all** to view all app insights by category.

To update the app categorization database, go to System settings.



On many devices, but not all, it also includes information on storage volume, data types, volume of storage per data type, and free data.

6. Click **Continue**. The following window appears.

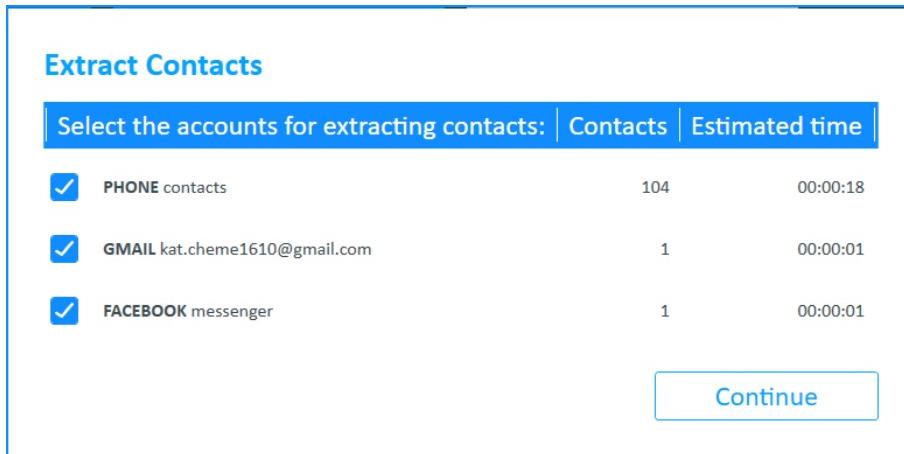


7. Data can be extracted from the Device, SIM and Memory Card of the device. Select from which memory you want to extract.
8. Different data types can be extracted. Select which data types you want to extract. In the example above, music and ringtones are excluded and will not be extracted.

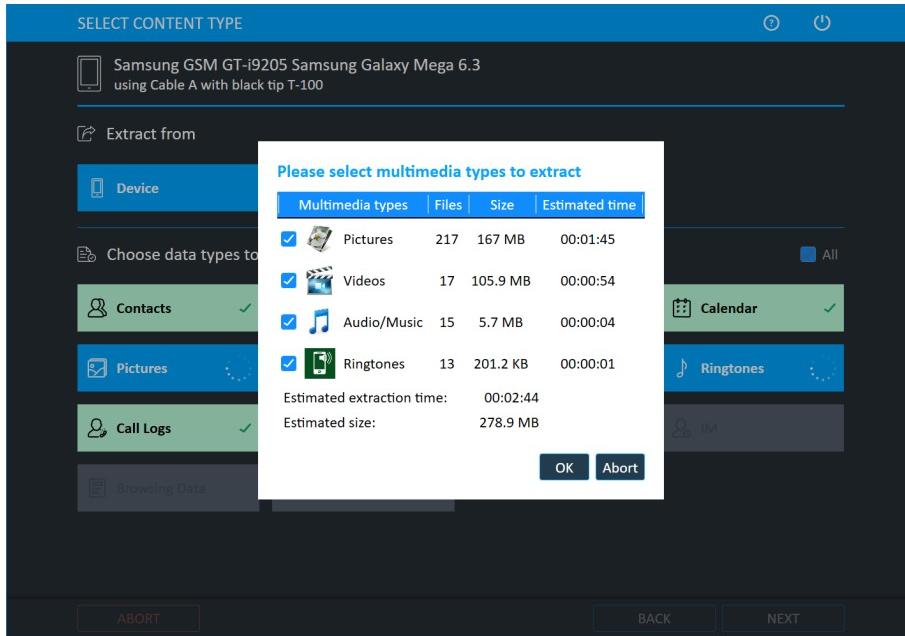


When Files is selected, UFED performs ADB backup to enable user data to be extracted.

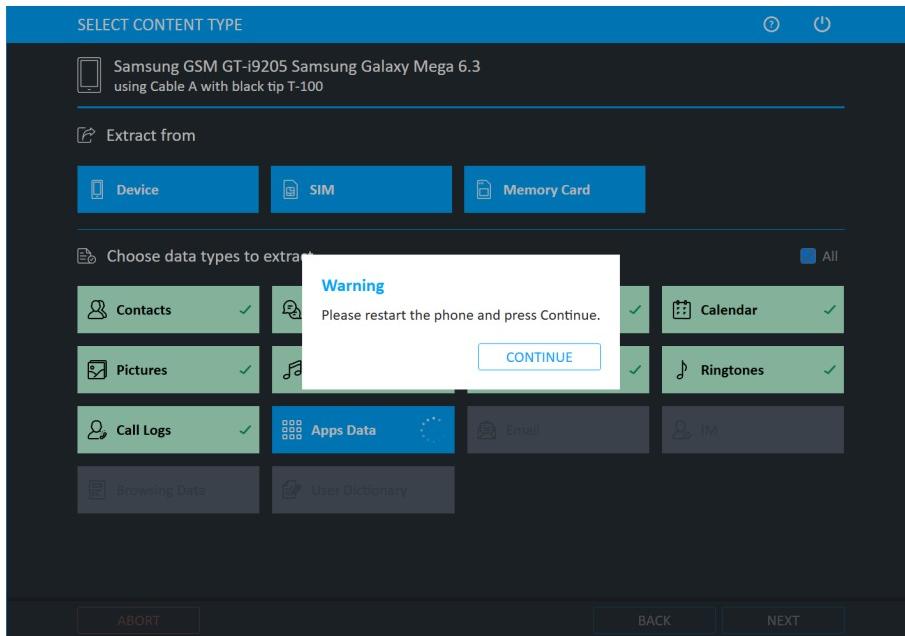
9. Click **Next**. The following window appears.



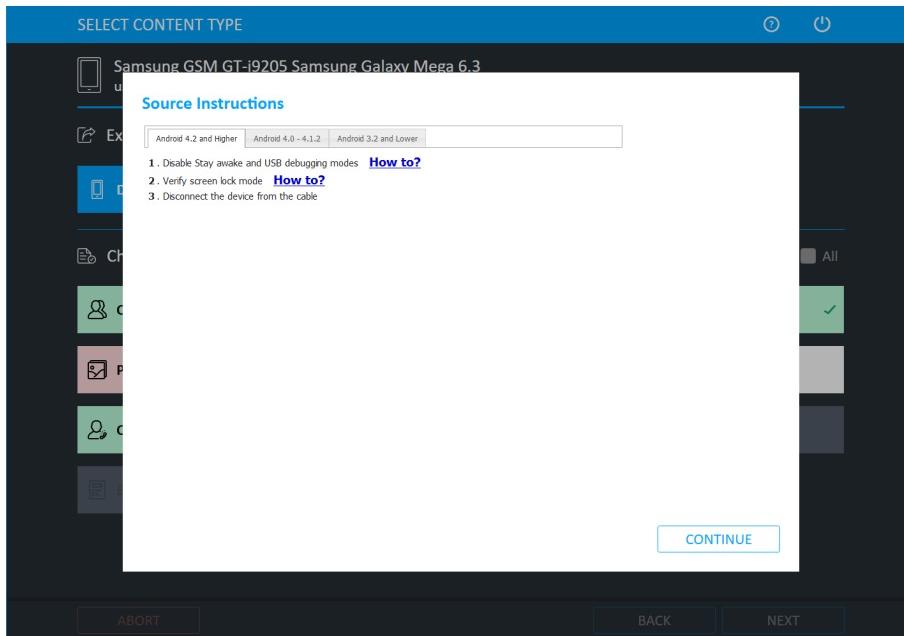
10. Select the required contacts to extract and click **Continue**. The extraction process starts.



11. Click OK. The following window appears.



12. If required, restart the device then tap Continue. When the extraction is complete and if required, the Source Instructions window appears (this depends on the device model). The following window appears.



13. Follow the instructions to return the mobile device settings to the original settings, and then click **Continue**.

EXTRACTION SUMMARY			
Extraction completed successfully			
Phonebook	106	SMS	31
MMS	0	Email	NOT SUPPORTED
IM	NOT SUPPORTED	Calendar	0
Pictures	217	Audio/Music	15
Videos	17	Ringtones	13
Call Logs	8	Browsing Data	NOT SUPPORTED
User Dictionary	NOT SUPPORTED	Apps Data	5,847 files
<a href="#">Open with UFED Physical Analyzer</a> <a href="#">Show in Folder</a>		<a href="#">OPEN</a>	<a href="#">ADDITIONAL EXTRACTIONS</a>
		<a href="#">FINISH</a>	

14. Click **Open Preview Report** to view an HTML preview report (Logical extractions only) that includes information about the device and the extraction, click **Open with Physical Analyzer** to open the extraction in Physical Analyzer, click **Show in Folder** to open the folder where the UFD extraction file is located, click **Additional Extractions** to add additional extraction types for the same device, or click **Finish** to end the process and return to the Home screen.

An example of a preview report is shown next.

Phone Examination Preview Report Properties	
Selected Manufacturer:	Samsung GSM
Selected Model:	GT-i9205 Samsung Galaxy Mega 6.3
Detected Manufacturer:	samsung
Detected Model:	GT-i9205
Revision:	4.4.2 KOT49H I9205XXUDOA1
IMEI:	357426050266879
Extraction start date/time:	15/02/2017 11:58:56
Extraction end date/time:	15/02/2017 12:14:59
Phone Date/Time:	15/02/2017 11:59:21 (GMT+2)
Connection Type:	USB Cable
UFED Version:	Product Version: 6.1.0.13 , Internal Build: 4.5.2.13 UFED
UFED S/N:	560AKCLQPHAYYOKSFNC
Note: This device is using client in order to communicate with UFED	
For complete analysis and advanced reporting, open in UFED Physical/Logical Analyzer.	
<b>•Generic Extraction Notes:</b> +ZZ – Extracted phone time stamp time zone is expressed in quarters of an hour Last IMEI digit might be incorrect. Please check manually on the device.	

### 3.1. The extracted data folder

At the end of the data extraction process, the extracted data is saved in the location you selected.



The extracted data folder is named "UFED" with the selected device name, the IMEI/MEID info. and the extraction date. For example, "UFED Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 2014\_11\_10 (0001)"

The extracted data folder contains:

- » Multimedia files folders named Audio, Images, Ringtones, and Video folders, containing each of the respective type of media files.
- » Phone extraction report files in HTML and XML formats. (One HTML report per content type)
- » Cellebrite UFED Manager files of the extracted calls log (\*.clog), phonebook (\*.pbb), SMS messages (\*.sms), and calendar (\*.cal) Email(\*.Email), MMS(\*.MMS) and IM(\*.IM) data.
- » UFD file.



UFED Manager files are generated only for data types that contain items.

The XML file can be viewed by both Logical Analyzer and Physical Analyzer.

## 4. Settings

The settings screen provides access to a set of functional and behavioral setup options used to control the functionality and usability of Cellebrite UFED.

To access the settings screen, click the menu icon in the application taskbar and select Settings..

The settings are grouped in the settings screen in the following tabs:

- » [General settings \(on the next page\)](#)
- » [Report settings \(on page 65\)](#)
- » [System settings \(on page 69\)](#)
- » [License settings \(on page 70\)](#)
- » [Version details \(on page 79\)](#)
- » [Activity Log \(on page 89\)](#)
- » [Users permissions \(on page 92\)](#)

The settings screen opens on the **General** tab.



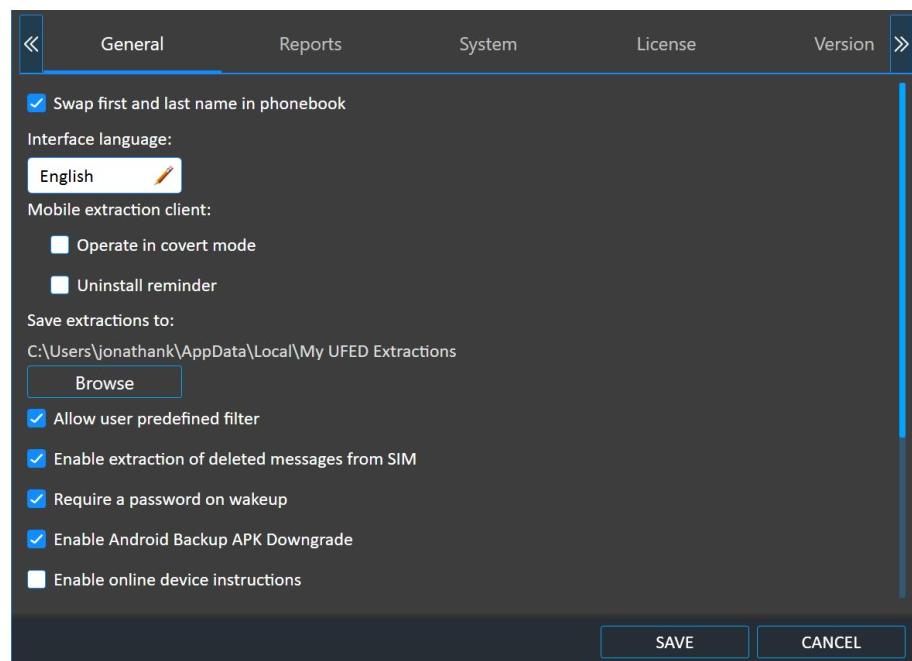
When using the Cellebrite Commander, some or all of these settings may be managed by Cellebrite Commander.



Changes that are made to the settings via Cellebrite Commander or manually by a user, will affect all users on the same machine.

## 4.1. General settings

The settings screen opens on the **General** tab.



The **General** tab provides access to the following functions and settings:

Setting	Description	Default
Swap first and last name in phonebook	Swaps the first and last name in phone book entries.	Selected
Interface language	Changes the interface language. For more information, see <a href="#">Changing the application interface language (on page 60)</a>	English
Operate in covert mode	Renames the application client name from "Cellebrite.sis/exe" to "AAA.sis/exe".	Selected
Uninstall reminder	When enabled, the Cellebrite UFED prompts you to uninstall the client from the examined device.	Selected

Setting	Description	Default
Save extractions to	Sets the location where extractions are saved. For more information, see <a href="#">Changing the extraction location (on page 64)</a>	
Allow user predefined filter	Displays the timeframe and select parties windows during an extraction. This check box is not enabled by default. For more information on the User predefined filter, see <a href="#">User predefined filter (on page 33)</a> .	Selected
Enable extraction of deleted messages from SIM	Extracts deleted messages from a SIM. This check box is selected by default.	Selected
Require a password on wakeup	Requires the user to enter a password when Cellebrite UFED is in sleep mode.	Selected
Enable Android Backup APK Downgrade	Enables the Android Backup APK Downgrade method. This check box is selected by default.	Selected

Setting	Description	Default
<b>Enable online device instructions</b>	<p>Displays the online device instructions instead of the offline device instructions. This check box is not enabled by default.</p> <div data-bbox="750 369 1240 1003" style="border: 1px solid #0072BD; padding: 10px;">  This setting is for the Waiting for Device instructions, which explains how to connect a source device to Cellebrite UFED. If you have network performance issues when using the online device instructions, clear this check box.       </div>	Not selected
<b>Show device restart alerts</b>	<p>Displays device restart alerts during the extraction process. This check box is not selected by default.</p>	Not selected
<b>Cable and Tip mode</b>  <b>Include Case details screen</b>	<p>Indicates the cable or tip to be used during the extraction.</p> <p>Displays the Case details window during the extraction process. This check box is not enabled by default. For more information, see <a href="#">Case details (on page 37)</a>. If this check box is selected, you can also optionally display the extraction folder name according to the case details. The default is according to the device model name.</p>	Tip  Not selected

Setting	Description	Default
Show investigation notes	Displays the Investigation notes widget, which enables you to add pictures, screen shots and text to document the investigation. See <a href="#">Investigation notes (on page 38)</a> .	Not selected
Include camera screen	Displays the camera window during the extraction process. This check box is not enabled by default.	Not selected
Automatically open extractions with Physical Analyzer	If installed, the extraction will be opened automatically in Physical Analyzer.	Not selected
Choose additional logo	Select an additional logo that will be displayed in the title bar of the home screen.	
Video quality	Set the video quality of the Cellebrite UFED camera to Best (1920 x 1280), Normal (1024 x 1280 default) or Low (640 x 480).	Normal
Enable device info (Advanced logical)	Displays the Device Info window during the Advanced Logical extraction. This window provides information on the device data, before performing an Android extraction.	Selected

#### 4.1.1. Changing the application interface language

1. Click the language field.

## Interface language:

English



The Select Language screen appears with the current language selected. (In this case, English).

Select Language

English (English)	Arabic (العربية)	Chinese (Traditional) Legacy (中文(繁體) 舊版)
Croatian (Hrvatski)	Czech (Čeština)	Danish (Dansk)
Dutch (Nederlands)	French (Français)	German (Deutsch)
Greek (Ελληνικά)	Hindi (हिन्दी)	Hungarian (Magyar)

1 / 3

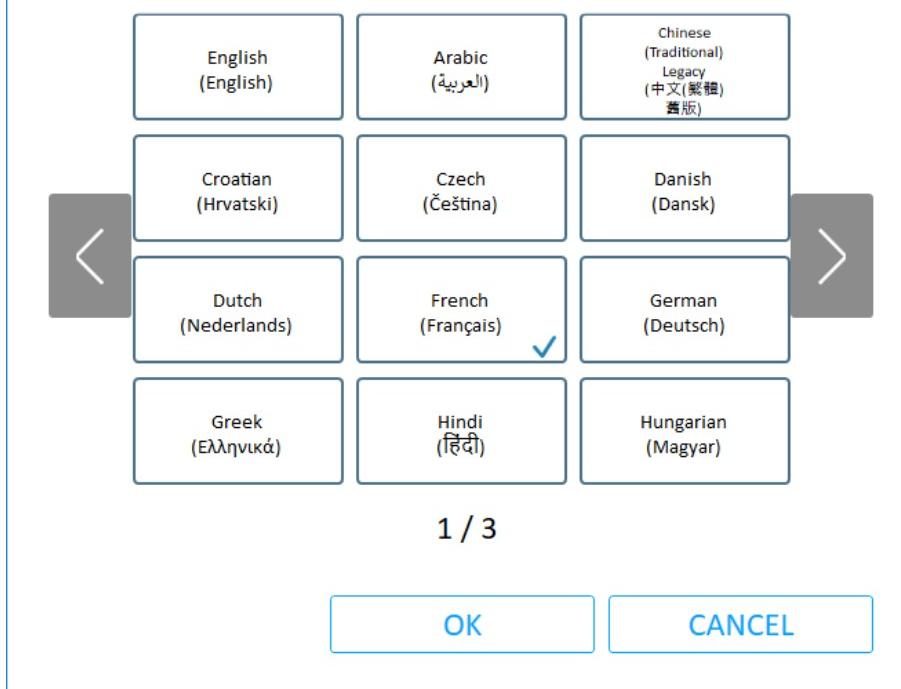
OK      CANCEL



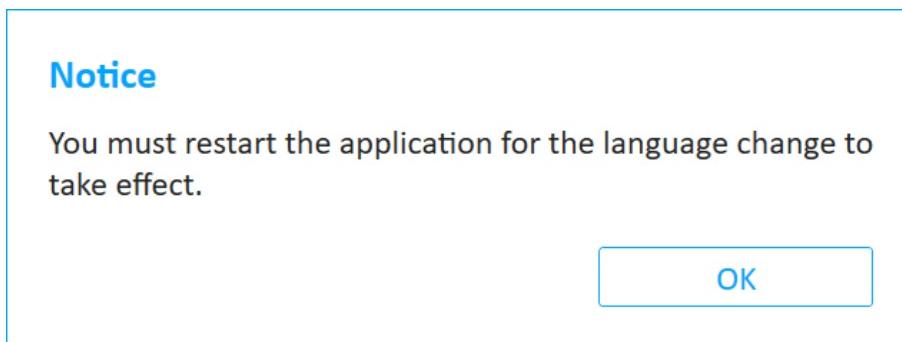
Use the arrows to scroll through the list of available interface languages.

2. Click the required language.

## Select Language



The following message appears (in the selected language):



3. Click OK.

The **General** tab appears with the language of choice in the Interface language field.

4. Click **Save** to close the Settings panel.
5. To restart the application:



- To close the application, click  in the application taskbar.
- To restart the application, do one of the following:
  - » Click the application shortcut icon located in the UFED shortcuts panel at the right of the screen.
  - » Double-click the Cellebrite UFED icon located on the Desktop.

- » Click Start > Cellebrite UFED
- » Click Start > All Programs > Cellebrite Mobile Synchronization > Cellebrite UFED.

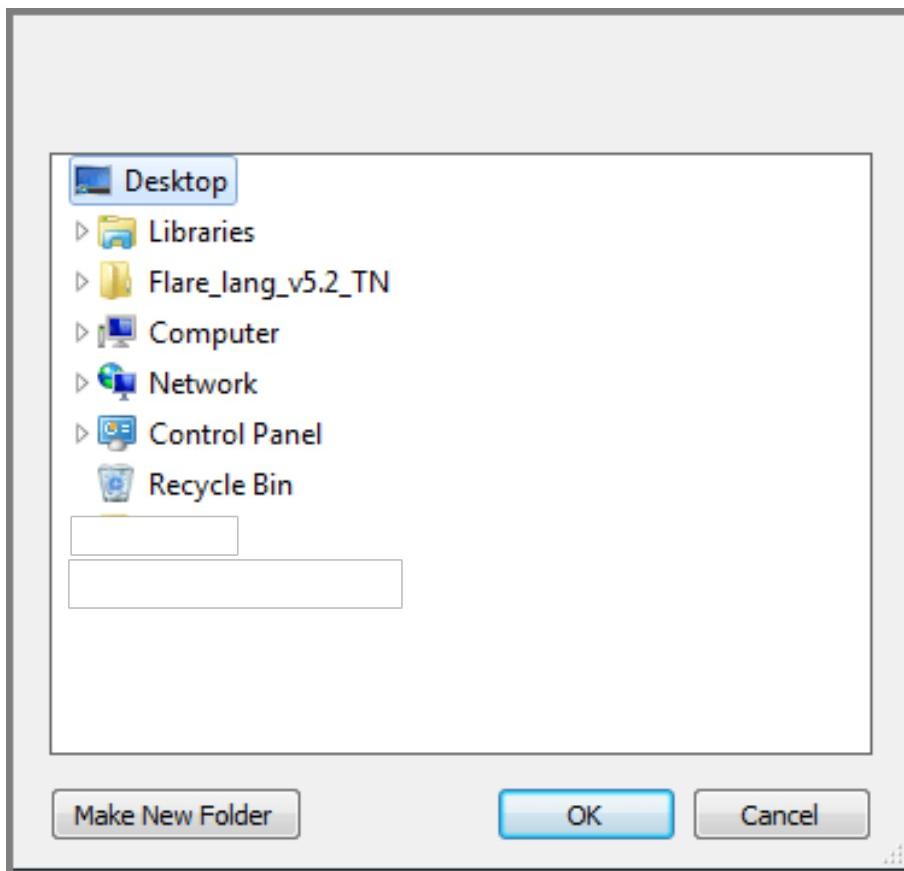
Cellebrite UFED starts in the selected language.



If Simplified Chinese is added to the Cellebrite UFED license, you will need to restart the application before the change will take effect.

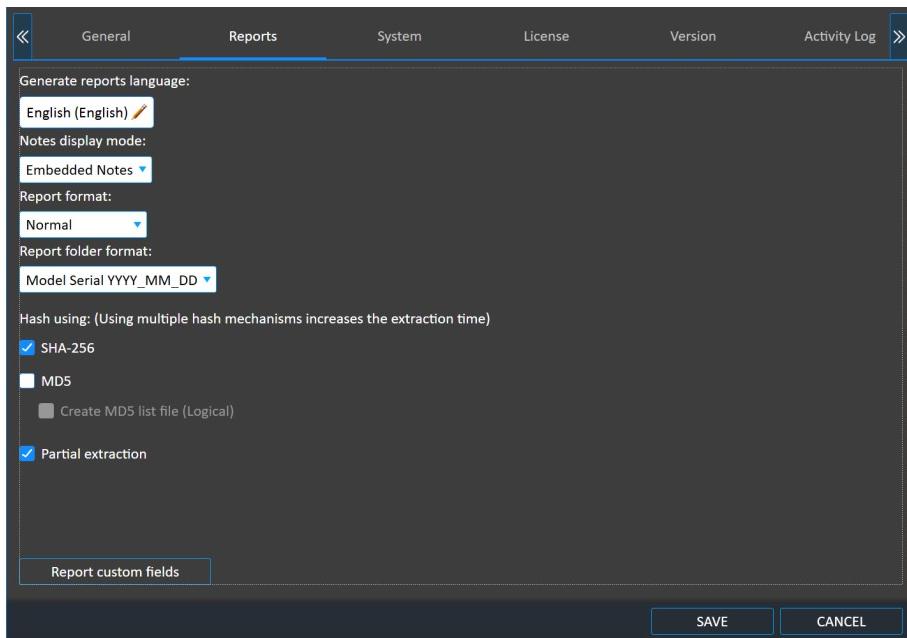
#### 4.1.2. Changing the extraction location

1. In the Save extractions to area, click **Browse**. The Browse for folder dialog appears.



2. Select the folder where you want to save the extraction files, and click **OK**.

## 4.2. Report settings



To set the report settings:

1. Access the **Settings > Reports** tab.
2. To set the generated reports language, click  next to **Generate Reports Language**, and select the desired language.
3. To set how the known issues notes about the extracted device are logged in the generated report, click  next to **Note display modes**, and select one of the following:
  - » **Disable** – Do not include device specific notes in the report.
  - » **Separated Notes** – Add all the device specific notes at the end of the report.
  - » **Embedded Notes** – Device-specific notes follow the content type they refer to in the report.
4. To set the generated reports visual formats, click  next to **Report format**, and select one of the following:
  - » **Normal** – The standard report structure, suitable to standard display screens.
  - » **Compact** – A compact report structure, suitable for devices with a small display area.

5. To set the generated reports folder name formats, select  next to **Report folder format**, and select one of the following:
  - » **Model Serial YYYY\_MM\_DD** – The folder name is constructed from <the model name> <the model serial> <the year in 4 digits>\_<the month in 2 digits>\_<the day in 2 digits>
  - » **YYYYMMDD Model Serial** – The folder name is constructed from <the year in 4 digits><the month in 2 digits><the day in 2 digits> <the model name> <the model serial>
6. Select or clear **Hash using MD5** to toggle the display of the MD5 values which are generated for each file in the extracted data. This increases the time required to complete the extraction.
7. Select **Create MD5 list file** to generate a Checksums.md5 file that contains all the generated MD5 values of the extracted data.
8. Select or clear **Hash using SHA-256** to toggle the display of the SHA-256 values which are generated for each file in the extracted data.
9. Select or clear **Partial Extraction**, in the event of an extraction error, whether or not to include the partially extracted data up to the error point in the generated report.
10. Click **Report custom fields** to add, remove and edit report fields. For more information, see [Managing report fields \(on the next page\)](#).
11. To set a field as required, click the field in the **Required** column.
12. Click **Save**.

#### 4.2.1. Managing report fields

1. Click **Report custom fields** to customize the report by defining additional fields which will be filled at the end of the extraction.

**Manage report custom fields**

Field Name	Required
Case number	
Examiner name	
Department	
Address	
Notes	

**Add**  
**Delete**  
**Edit**

**Save**    **Cancel**

2. To add a new field:

- a. Click **Add**.

**Manage report custom fields**

Field Name	Required
<input type="text"/>	<input checked="" type="checkbox"/>

**Save**    **Cancel**

- b. Enter the field name in the **Field Name** box.



To display the keyboard, click **Keyboard**.

- c. To set the field as mandatory, select **Required** next to the field name.
  - d. Click **Update**, or to exit without saving, click **Cancel**.
3. To add additional fields, repeat step 2.
  4. To edit an existing field:
    - a. Click the field in the list, and click **Edit**.
    - b. Repeat steps 2b-2d.



You cannot edit the field name of a default custom field.

5. To delete a field:
  - a. Click the field in the list, and click **Delete**.

### Delete custom report field

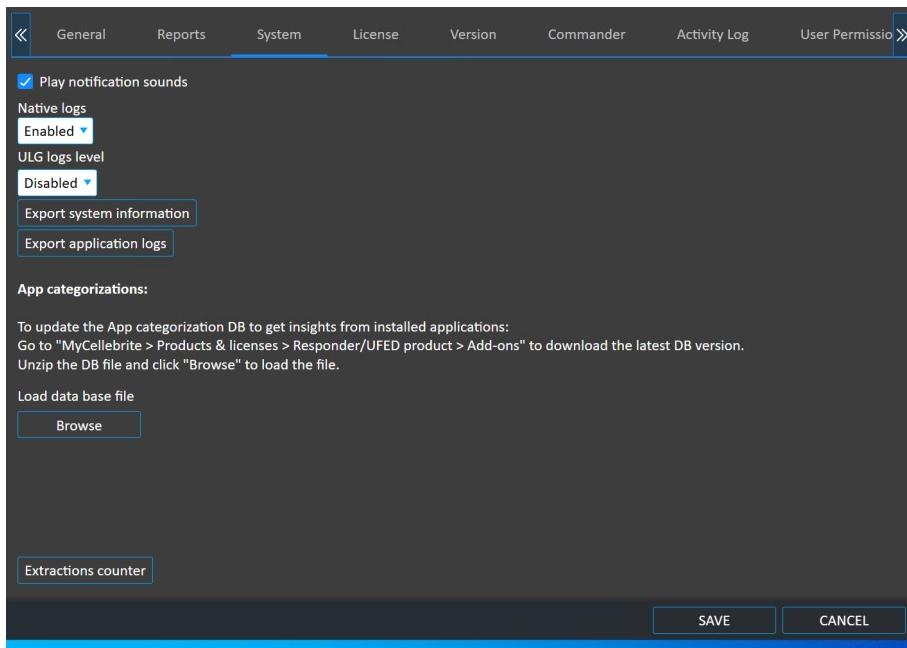
Are you sure you want to delete 'Notes' field?

YES

NO

- b. In the confirmation message, click **Yes**.
6. Click **Save** in the **Reports** tab.

## 4.3. System settings



Define the following additional settings in the System tab:

- » To set Cellebrite UFED to alert you when your attention is required, such as when it is waiting for your input or when an extraction fails, select **Play notification sounds**.
- » To change the **ULG logs level**, select one of the following:
  - » **Disabled** – The system will not generate log files.
  - » **Detailed** – The system will generate detailed log files. The transaction will be slower in order to write to the log. Recommended in case of debugging/error situation.
- » To export system information, click **Export system information**.
- » To save the application logs, click **Export application logs**.
- » To update the App categorization DB to get insights from installed applications, go to **MyCellebrite > Products & licenses > Cellebrite UFED 4PC > Add-ons** to download the latest DB version. Unzip the DB file and click **Browse** to load the file.
- » To monitor device usage, click the **Extractions counter**. This counts the number of extractions performed by Cellebrite UFED. Transactions include all extractions per type and device tool actions. The counters are managed locally and can be reset.

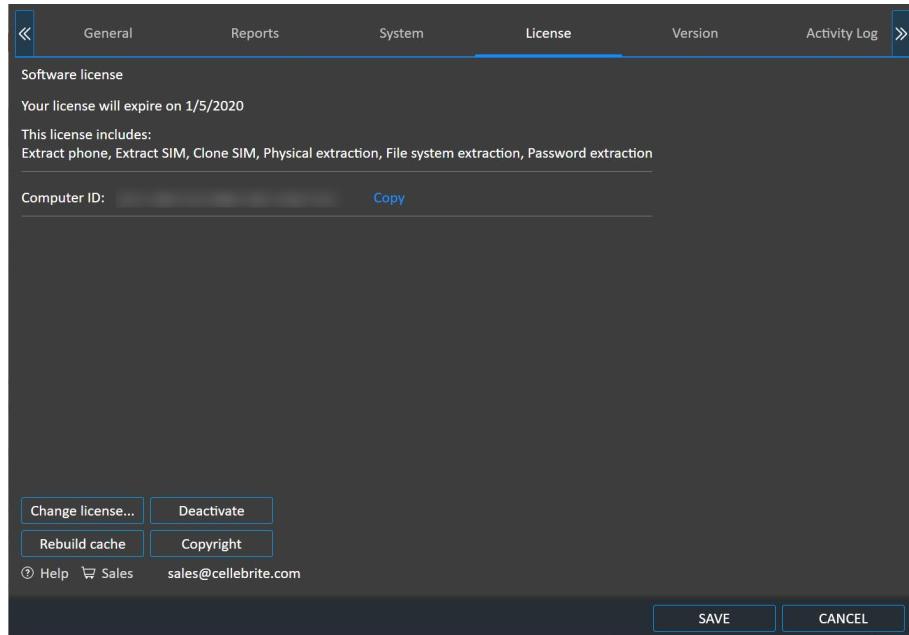


The password to reset the Extractions counter is the Computer ID or dongle serial number (displayed in the **License** tab).

## 4.4. License settings

Change the license type in the **License** tab.

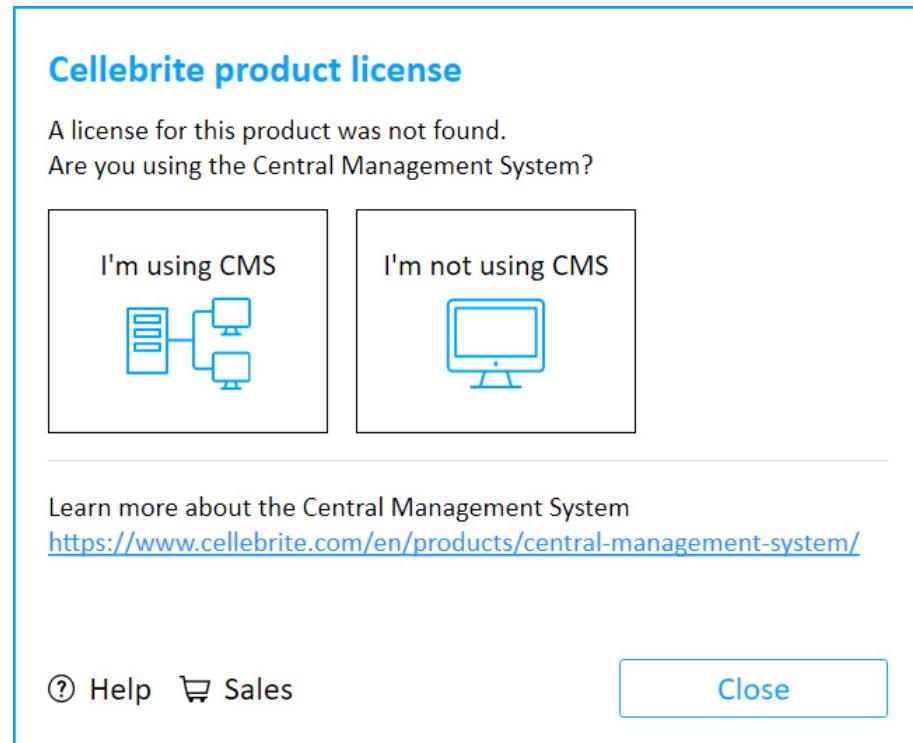
The current license type is displayed.



To change the license type, follow the instructions in [Activating the license \(on page 21\)](#).

#### 4.4.1. License not found

If a license cannot be found the following window appears.



If you are using Cellebrite Commander:

1. Click I'm using Cellebrite Commander. The following window appears.

## Cellebrite product license

Connect to your Centralized Management System (CMS) server

### CMS Server:

If you have a license dongle, connect it before validating

### Status:

Connection not initiated

2. Connect the license dongle before validating.
3. Enter the Cellebrite Commander Server information. For more information on entering the information in this window, see [Connect a Cellebrite UFED device to Cellebrite Commander \[on page 82\]](#).
4. Click Validate.

### If you are not using Cellebrite Commander:

1. Click I'm not using Cellebrite Commander. The following window appears.

## Cellebrite product license

Select your license type:

Dongle



Software



[? Help](#) [Sales](#)

[Back](#)

[Close](#)

2. Select your license type.

## 4.4.2. Updating a dongle license online

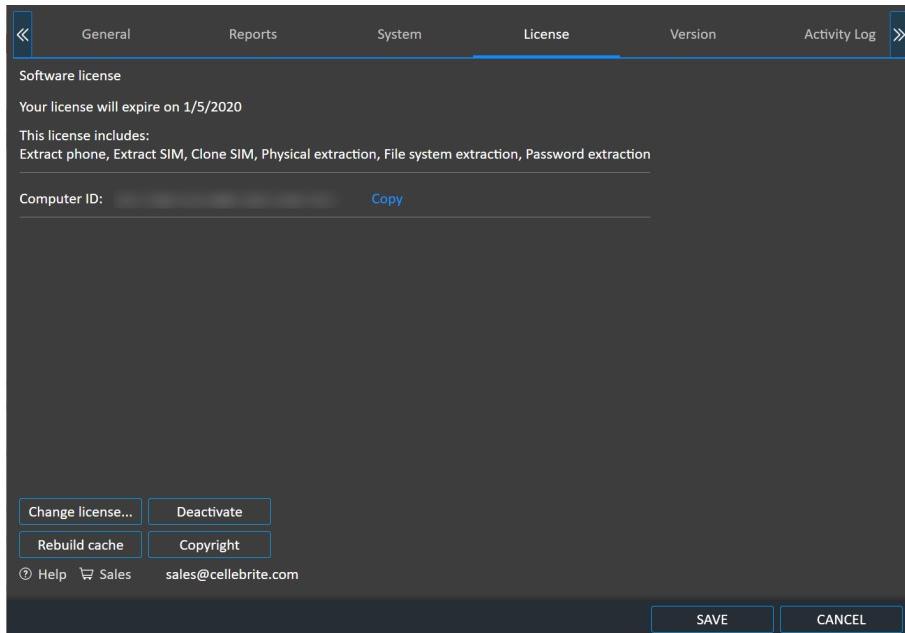
When an Internet connection is available, you can update the dongle license directly from Cellebrite UFED.

### To update a dongle license online:

1. Contact your Cellebrite sales representative to renew or update the dongle license. Once the license is approved, you can then proceed with the following steps.



2. From the Home screen, click  and then click the License tab. The following window appears.



3. Click **Change license**. The following window appears.

## Cellebrite product license

Select your license type:

Dongle



Software



② Help ⚒ Sales

[Close](#)

4. Click Dongle. The following window appears.

## Cellebrite product license

Connect the dongle to a USB port on your computer.  
It will be detected automatically.

If you connected a dongle and it still doesn't work, [contact Cellebrite support](#).  
[Load license file](#) [Update license \(online\)](#)

② Help ⚒ Sales

[Back](#)

[Close](#)

5. Click Update license (online).
6. Click OK to complete the process.

#### 4.4.3. Updating a software license online

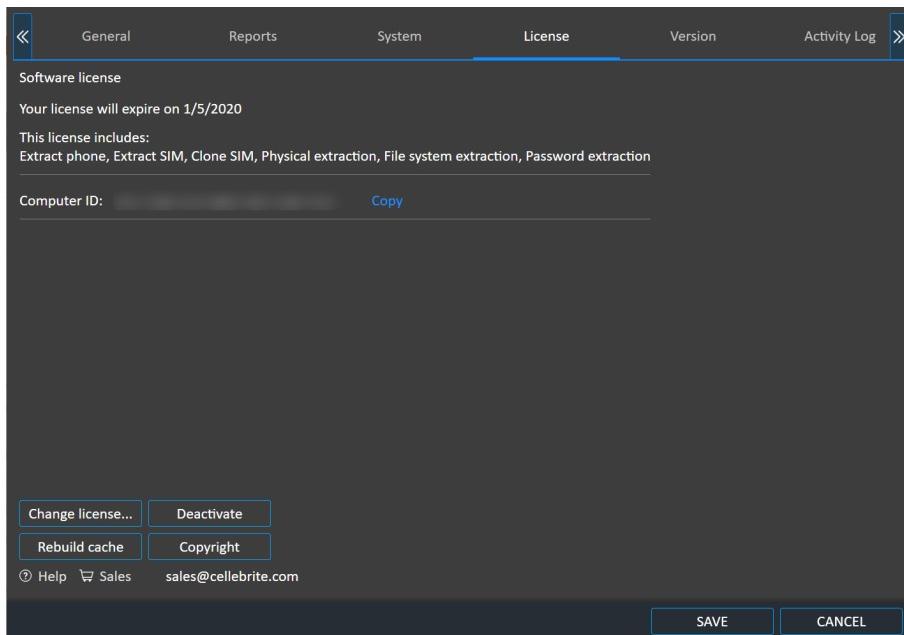
When an Internet connection is available, you can update a software license directly from Cellebrite UFED.

##### To update a software license online:

1. Contact your Cellebrite sales representative to renew or update the dongle license. Once the license is approved, you can then proceed with the following steps.



2. From the Home screen, click  and click the **License** tab. The following window appears.



3. Click **Change license**. The following window appears on Cellebrite UFED.



For Cellebrite UFED Touch, accept the Cellebrite UFED License Agreement and skip to step 6.

## Cellebrite product license

Select your license type:

Dongle



Software



[② Help](#) [🛒 Sales](#)

[Close](#)

4. Click Software. The following window appears.

### Cellebrite product license

Software license

Your license will expire on 1/5/2020

This license includes:

Extract phone, Extract SIM, Clone SIM, Physical extraction, File system extraction, Password extraction

Computer ID: N3Y-2EW-PID-WNB-ZWJ-X2W-YG4

[Copy](#)

[Update software license](#)

[② Help](#) [🛒 Sales](#)

[Back](#)

[OK](#)

5. Click Update software license. The following window appears.

## Cellebrite product license

Already have a license file?

[Load license file](#)

[Load from the web](#)

Need to download your software license?

[Go to MyCellebrite](#)

Computer ID: N3Y-2EW-PID-WNB-ZWJ-X2W-YG4

[Copy](#)

[② Help](#) [Sales](#)

[Back](#)

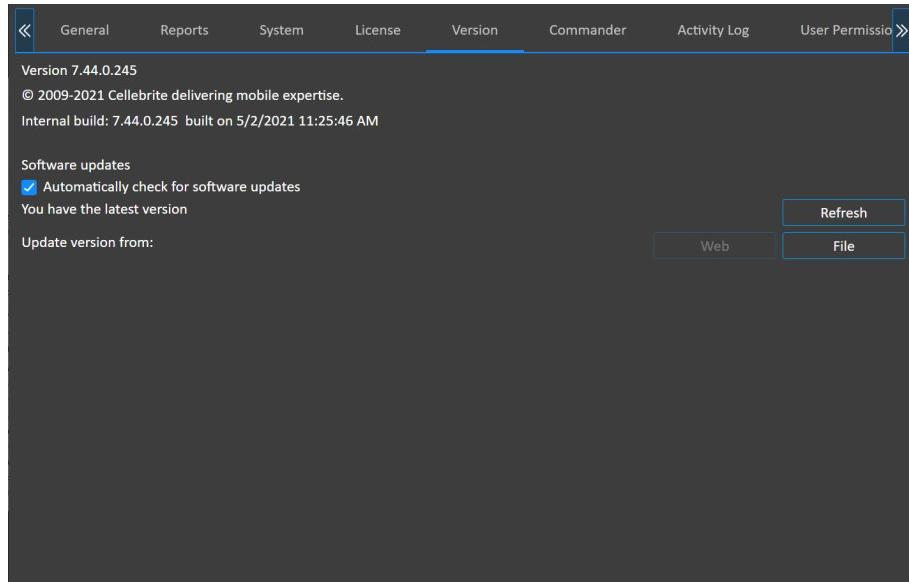
[Close](#)

6. Click Load from the web.
7. Click OK in the Cellebrite product license window to complete the process.

## 4.5. Version details

The version tab displays information about the Cellebrite UFED version and build.

Under Software updates, select the check box to automatically check for software updates.



### 4.5.1. Updates and versions

When Cellebrite UFED is connected to the Internet, automatic notifications appear in the event of updates and new versions of the application.

- » Click **Refresh** in the Settings > **Version** tab to update the information available on the screen.

**To install a newer version of the Cellebrite UFED application via the web:**



Before using this option, ensure that the unit is connected to the network.

- » In the **Settings > Version** tab, in the **Version** area, click **Web**.

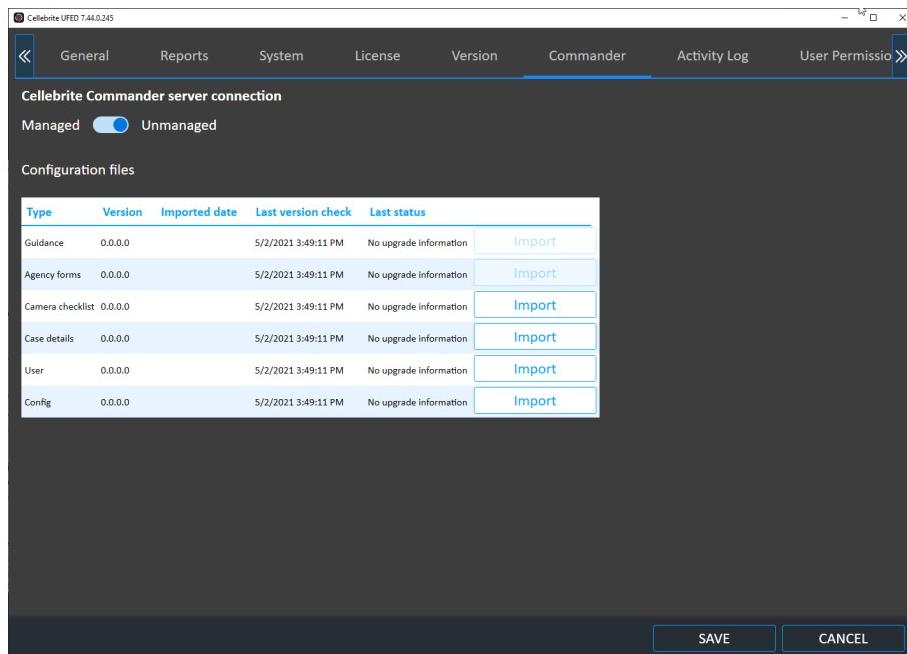
The application is upgraded to the latest version available on the Cellebrite Commander (if relevant) or Cellebrite download server.

**To install a newer version of the Cellebrite UFED application using the file option:**

1. Download the latest application version from your account in MyCellebrite, and save it to the specified directory on the PC or external device.
2. In the **Settings > Version** tab, in the **Version** area, click **File**.
3. Select the directory where you saved the file and then click **Open**.

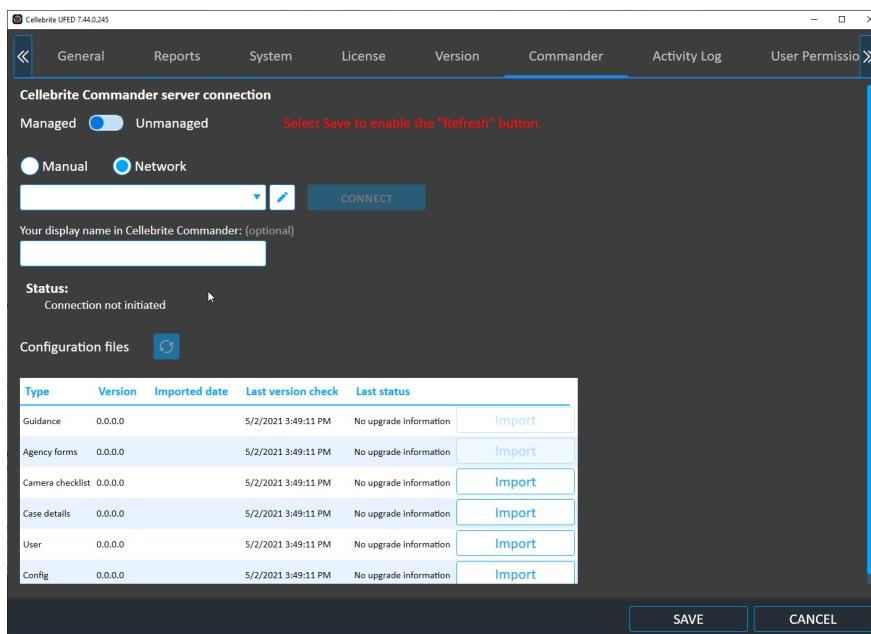
## 4.6. Commander settings

This tab can be used to manage and control deployed devices and systems via Cellebrite Commander. For more information, refer to the Cellebrite Commander manual.



If your organization is using Cellebrite Commander:

- » Click Managed mode.





For more information on setting up connectivity with Cellebrite Commander, see [Connect a Cellebrite UFED device to Cellebrite Commander \(on the facing page\)](#).



Cellebrite UFED 4PC checks for configuration file changes by default every 5 minutes.

### If you are not using Cellebrite Commander:

- » Verify that **Unmanaged mode** is selected.



You can also manually import configuration and settings files into the system and check for software updates.

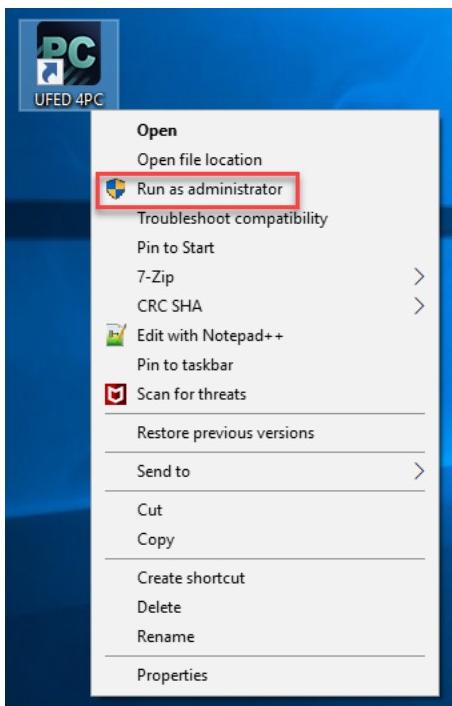
For more information on manually importing files, see [Importing settings and configuration files \(on page 84\)](#).

#### 4.6.1. Connect a Cellebrite UFED device to Cellebrite Commander

Cellebrite UFED devices will automatically detect when a new Cellebrite Commander server is added to their subnet and prompt the user to connect automatically. If necessary, it is also possible to connect a Cellebrite UFED device to Cellebrite Commander manually.

##### To connect a Cellebrite UFED device to Cellebrite Commander automatically:

1. Preliminary step (Only applies to Cellebrite UFED 4PC and Cellebrite Responder on a PC):  
Right-click on the application shortcut and select **Run as Administrator**



Enable Admin permissions in order to allow the Cellebrite UFED device to automatically download the SSL certificate. This will ensure secure SSL communication between a managed Cellebrite UFED unit and Cellebrite Commander server. To enable the download of certificates, make sure the setting is enabled in Cellebrite UFED 4PC Settings.

2. Restart the Cellebrite UFED unit.
3. The unit will automatically detect the Cellebrite Commander server and prompt the user to connect.
4. After the unit connects to the Cellebrite Commander server, it will automatically switch to managed mode and download the secure SSL certificate.



If more than one Cellebrite Commander is detected, the user can choose from the list of servers.

## To connect a Cellebrite UFED device to Cellebrite Commander manually:

1. Go to **Settings > Commander**. The following window appears.

The screenshot shows the 'Cellebrite Commander server connection' settings page. At the top, there is a toggle switch between 'Managed' (selected) and 'Unmanaged'. Below it, there are two radio buttons: 'Manual' (selected) and 'Network'. A text input field labeled 'Enter FQDN' contains 'Responder 7.40.0.33 test'. To the right of this field is a blue 'CONNECT' button. Below the FQDN input, there is a placeholder text 'Your display name in Cellebrite Commander: (optional)' followed by a text input field containing 'Responder 7.40.0.33 test'. Under the heading 'Status:', a green dot indicates 'Connected to Cellebrite Commander'. At the bottom, there is a section titled 'Configuration files' with a table showing various items and their status. The table has columns: Type, Version, Imported date, Last version check, and Last status. Each row has a blue 'Import' button. The table data is as follows:

Type	Version	Imported date	Last version check	Last status	Action
Guidance	1.0.0.8	11/17/2020 14:31	11/19/2020 17:31	No upgrade information	Import
Agency forms	1.0.0.9	11/06/2020 08:56	11/19/2020 17:31	No upgrade information	Import
Camera checklist	1.0.0.4	11/06/2020 08:56	11/17/2020 16:16	Latest version	Import
Case details	1.0.0.5	11/04/2020 17:25	11/19/2020 17:31	Update downloaded	Import
User	1.0.0.22	11/06/2020 08:56	11/19/2020 17:31	Latest version	Import
Config	1.0.1.24	11/04/2020 18:08	11/19/2020 17:31	No upgrade information	Import

2. Select **Managed mode**.
3. Enter the FQDN (fully qualified domain name).
4. Click **Connect**. If the validation is successful, the status changes to **Connected to Cellebrite Commander**.
5. Click **Save**.

## 4.6.2. Importing settings and configuration files

You can use Cellebrite Commander to download initial export files, which can then be edited if necessary and manually imported into Cellebrite UFED. These files can also be set using Cellebrite Commander. For more information, refer to the Cellebrite Commander manual.

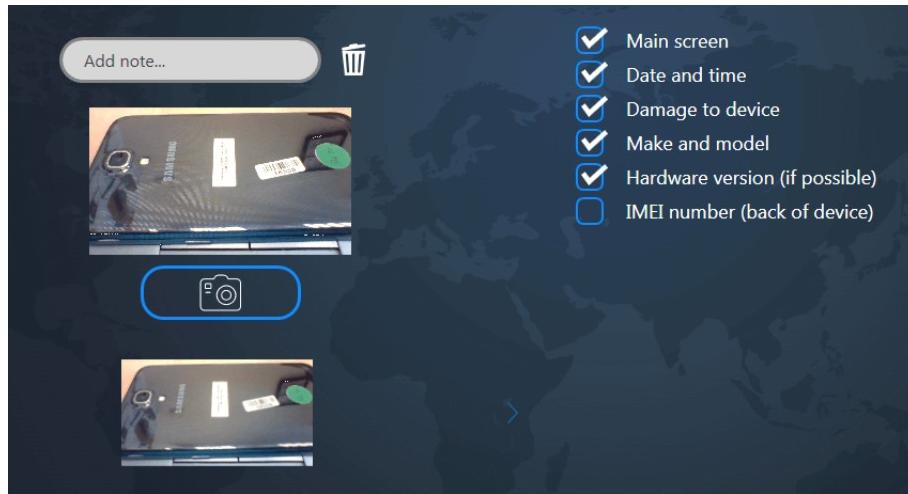
Cellebrite UFED can import the following type of settings and configuration files:

- » [Importing a camera checklist \(on the next page\)](#)
- » [Importing case details \(on page 86\)](#)
- » [Importing user management \(on page 88\)](#)
- » [Importing configuration files \(on page 89\)](#)

#### 4.6.2.1. Importing a camera checklist

The camera checklist enables you to upload an XML file that the user can use as a reference as to what pictures are required of the device. As the user completes each step, they can place a check mark next to the completed items.

An example is displayed next.



#### To manually import a Camera checklist file:

1. In the **Version** tab, click the **Import** button next to the setting file you would like to import. The following window appears.
2. Browse to the relevant file and click **Open**.
3. Click **OK** to update the application.

The following example shows the structure of the XML file.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CheckListData>
    <Version>1.0.0.48</Version>
    <CheckListItems>
        <CheckListItem>Main screen</CheckListItem>
        <CheckListItem>Date and time</CheckListItem>
        <CheckListItem>IMEI number</CheckListItem>
    </CheckListItems>
</CheckListData>
```

#### 4.6.2.2. Importing case details

You can import an XML file to change the options that appear in the Case Details window (see [Case details \(on page 37\)](#)).

##### To manually import a case details file:

1. In the Version tab, click the **Import** button next to the setting file you would like to import.
2. Browse to the relevant file and click **Open**.
3. Click OK to update the application.

The following example shows the structure of the XML file.

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CaseDetails>
    <Version>1.0.0.38</Version>
    <Fields>
        <Field>
            <Type>String</Type>
            <Caption>Case ID</Caption>
            <Mandatory>true</Mandatory>
            <AutoFill>true</AutoFill>
            <IsDefaultFolderName>true</IsDefaultFolderName>
        </Field>
        <Field>
            <Type>String</Type>
            <Caption>Seized by</Caption>
            <Mandatory>false</Mandatory>
            <AutoFill>false</AutoFill>
            <IsDefaultFolderName>false</IsDefaultFolderName>
        </Field>
        <Field>
            <Type>String</Type>
            <Caption>Crime type</Caption>
            <Mandatory>false</Mandatory>
            <AutoFill>false</AutoFill>
            <IsDefaultFolderName>false</IsDefaultFolderName>
            <Values>
                <Value>Armed Robbery</Value>
                <Value>Attempted Murder</Value>
                <Value>Child Exploitation</Value>
            </Values>
        </Field>
        <Field>
            <Type>String</Type>
            <Caption>Device owner</Caption>
            <Mandatory>false</Mandatory>
            <AutoFill>false</AutoFill>
            <IsDefaultFolderName>false</IsDefaultFolderName>
            <Values>
                <Value>Victim</Value>
                <Value>Suspect</Value>
                <Value>Witnessss</Value>
            </Values>
        </Field>
    </Fields>
</CaseDetails>

```

#### 4.6.2.3. Importing user management

Cellebrite Commander enables user authentication ensuring that only users with the right credentials can access the application. Access rights are further enforced by defining permission levels per profile.

##### To manually import a user management file:

1. In the **Version** tab, select the **Import** button next to the setting file you would like to import.
2. Browse to the relevant file and click **Open**.
3. Click **OK** to update the application.

#### 4.6.2.4. Importing configuration files

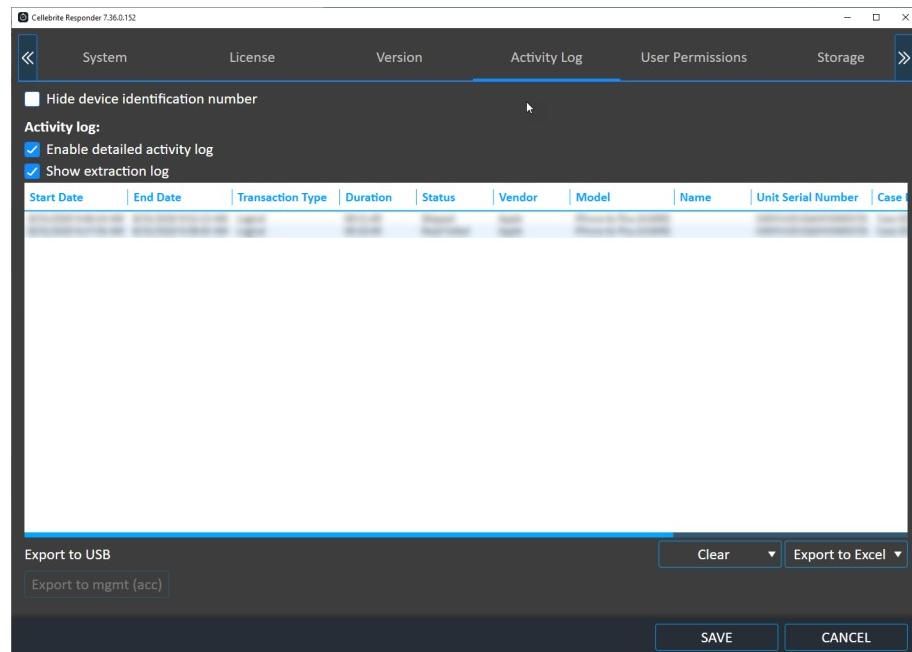
Configuration files enables you to import various settings into the system.

##### To manually import a configuration file:

1. In the Version tab, select the **Import** button next to the setting file you would like to import.
2. Browse to the relevant file and click **Open**.
3. Click **OK** to update the application.

## 4.7. Activity Log

The Activity Log lists all transactions performed by Cellebrite UFED. It includes information such as when the extraction started and ended, transaction type, duration, status, device vendor, device model, name, serial number of Cellebrite UFED, case ID, crime type, device owner, and who seized the device. You can also clear the activity log, export the activity data to a CSV file and show or hide the activity data.



### 4.7.1. Exporting metadata to Cellebrite Commander

If a Cellebrite UFED unit is used in an offline environment, you can export the usage metadata file. This file contains the following: Cellebrite UFED device information (e.g., MAC address, serial number, software version number), transaction start times and end times, source phone information (e.g., vendor, model name, IMEI, and OS), and type of information extracted (e.g., Phone memory, SMS memory, MMS, pictures, videos, audio). The exported

Zip file can then be manually imported into Cellebrite Commander. For more information, refer to the Cellebrite Commander manual.

### To export the metadata:

1. Connect or reconnect a USB flash drive to the Cellebrite UFED unit. The button is only available when a USB drive is connected.
2. Click the **Export to mgmt (acc)** button. The metadata can now be imported into Cellebrite Commander.



This button is only displayed if you are using the Managed mode (see [Version details \(on page 79\)](#)).

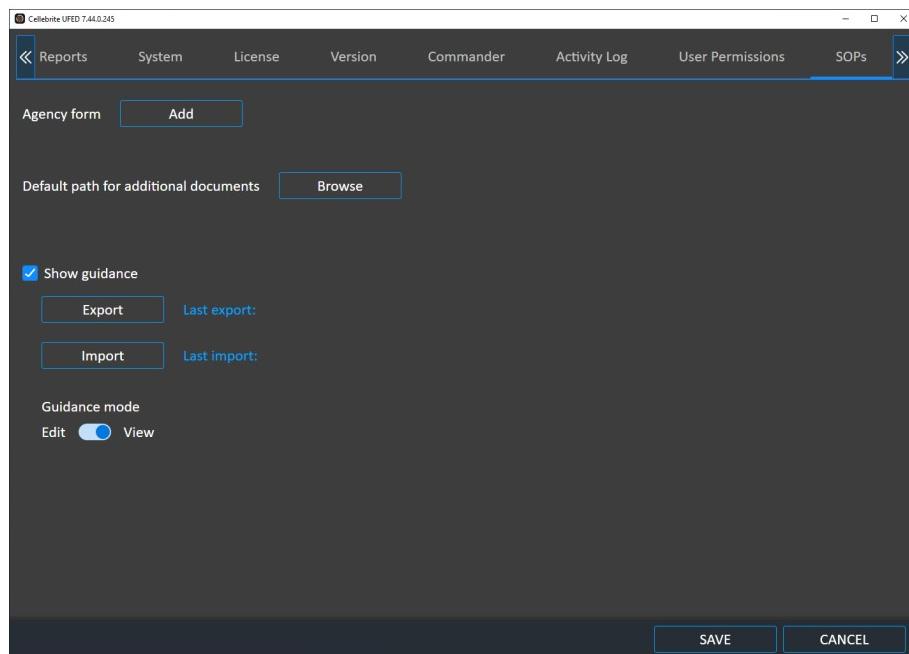


Exported data is removed from the Cellebrite UFED device and is not available for export again.

## 4.8. SOPs

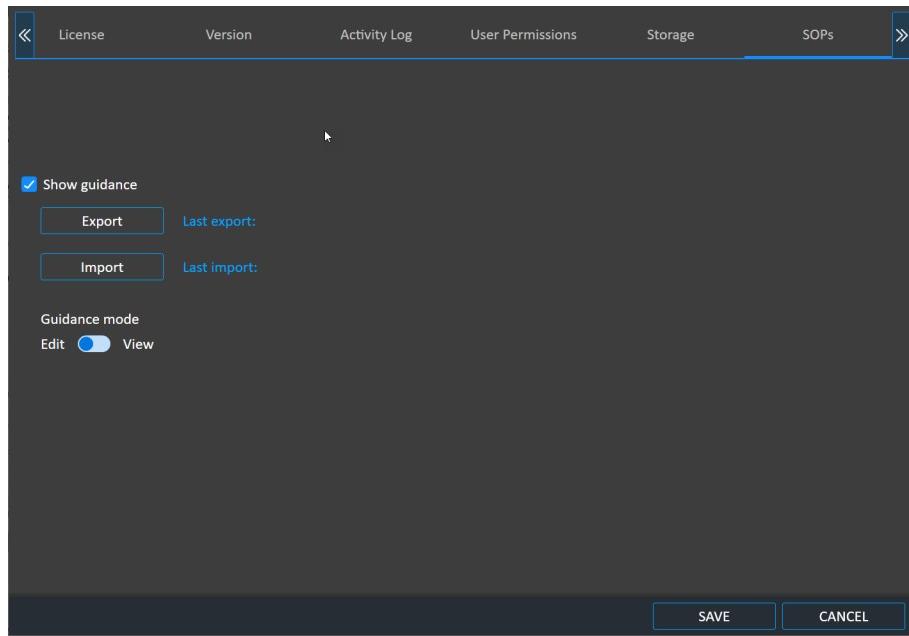
In the Settings > SOPs, you can manage the following:

- » Adding Agency forms.
- » Setting a default path for additional documents.
- » Managing Workflow guidance. See [Workflow guidance settings \(on the next page\)](#).



## 4.8.1. Workflow guidance settings

Manage Workflow guidance settings in **Settings > SOPs**.



The following settings can be found in the Workflow guidance settings:

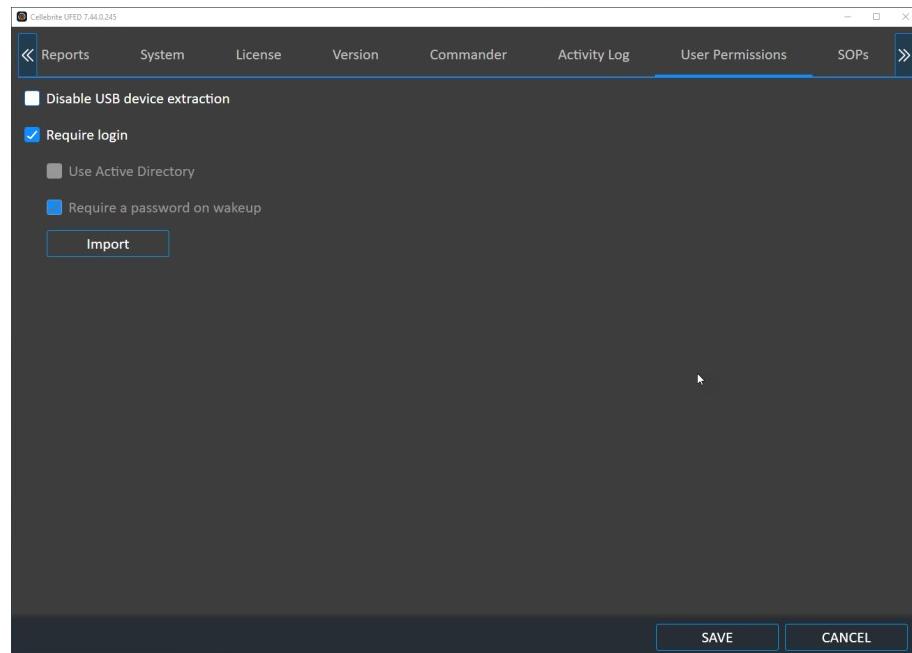
- » **Show guidance** - When selected, the guidance will appear in the system. Unselect this option to disable the guidance.
- » **Export** - Export guidance to be used in other UFED units.
- » **Import** - Import guidance file.
- » **Guidance mode** - Set the unit to work in either Edit or View mode.

## 4.9. Users permissions

Define and configure user authentication settings to ensure that only users with the right credentials can access the application. Access rights are further enforced by defining permission levels per profile.



User permissions can be set using Cellebrite Commander (refer to the Cellebrite Commander *manual*) or the UFED Permission Manager (see [Permission management \(on page 101\)](#)).



### To disable USB device extraction:

- » Select the **Disable USB device extraction** check box. The USB device option will not be available on the home screen.

### To import user permissions:

1. Run the Cellebrite UFED as an administrator.
2. Click Import. The following warning appears.

#### Warning

Warning: Importing Permissions will override all existing user permissions.  
Continue?

YES

NO

3. Click **Yes** and navigate to the directory where the permission management file (\*.cp) is located. For information on creating a permission management file, see [Using the Cellebrite UFED Permission Manager \(on page 101\)](#).
4. Click **Open** and then click **Save**.
5. Restart the Cellebrite UFED application, which will now prompt for login credentials.
6. Use one of the login credentials configured in the permission management file. For more information, see [Permission management \(on page 101\)](#).



Select the check box to require password on wakeup.

#### 4.9.1. Active Directory integration

Active Directory is a Microsoft product providing a range of directory-based identity-related services. It authenticates and authorizes all users and computers in a Windows domain type network, assigning and enforcing security policies for all computers and installing or updating software.

When a user logs in to the system, Active Directory checks the submitted password and determines whether the user is a system administrator or normal user before allowing the user to log in. Active Directory also enables the management and storage of information at the admin level and provides authentication and authorization mechanisms.

Use the Windows Active Directory account to enable *quicker and easier* login to your Cellebrite UFED applications. Cellebrite UFED can manage the permissions with two permissions levels:

- » Active Directory Groups
- » Active Directory Users with Commander roles

##### 4.9.1.1. Determining the Active Directory groups



When using the **Groups level**, the permissions are applied according to the Active Directory groups of which the users are members (directly and indirectly). When using the **Users level**, you first need to map the users to Cellebrite Commander, and then to the permissions applied according to the selected profile in Cellebrite Commander. For more information, see [To enable Active Directory \(on page 96\)](#).

If required, use the following procedure to determine all the Active Directory groups for a specific user.

1. To get a list of groups for a specific user, replace the **USERNAME** with the actual user name

Open up a command prompt (cmd.exe) and run:

```
gpresult /V /user USERNAME
```

2. The output will look like this (truncated with only the group info):

```
The user is a part of the following security groups
```

```
-----
```

```
Domain Users
```

```
Everyone
```

```
BUILTIN\Users
```

```
NT AUTHORITY\INTERACTIVE
```

```
CONSOLE LOGON
```

```
NT AUTHORITY\Authenticated Users
```

```
This Organization
```

```
LOCAL
```

```
Marketing
```

```
- - -  
Platforms Dev Team
```



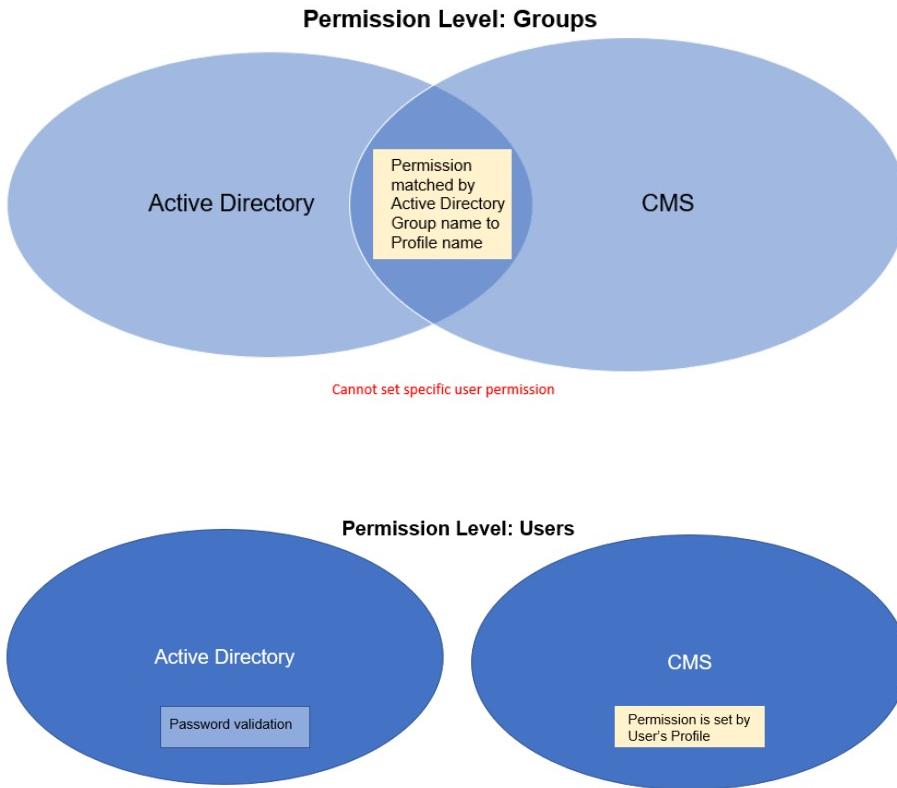
In the above example, you can see that this user is a member of several Active Directory (security) groups. In the following example we will use the "Platforms Dev Team" security group.



If a group is contained within another group, other commands (such as `whoami /groups`) will only display the groups of which the user is a direct member. Therefore, it is recommended to avoid `whoami` as an indicator.

#### 4.9.1.2. Using Cellebrite Commander

When using Cellebrite Commander, the system administrator needs to decide the permission management level. The possible levels are presented below:



#### 4.9.1.3. Initial setup

When Cellebrite Commander is used in conjunction with Active Directory, the following procedures are required for initial setup.

##### 4.9.1.3.1. Permission Level – Groups

The Cellebrite Commander administrator needs to:

1. Create *profiles* with the exact same name of the relevant Active Directory groups.
2. Publish the users and permissions to all the relevant Cellebrite UFED units.

Once Active Directory is set up, each login request via a Windows user will be sent to Active Directory before approval. Active Directory checks the user's permissions and notifies the Cellebrite UFED unit whether to approve or deny the login request based on the user profile permissions.



If the Cellebrite UFED units are offline, you will not be able to log in to the Cellebrite UFED unit. However, an ongoing session will not be disconnected if a disconnection occurred.



Should you choose not to work with Active Directory, the Cellebrite Commander administrator can regulate the users and permissions via Cellebrite Commander or the Cellebrite UFED Permission Manager.

#### 4.9.1.3.2. Permission Level – Users

The Cellebrite Commander administrator needs to:

1. Create *profiles* and set the permissions for each profile.
2. Import a CSV list of relevant *users* that matches the Users and Profiles settings in Cellebrite Commander.
3. Publish the users and permissions to all the relevant Cellebrite UFED units.

#### 4.9.1.4. To enable Active Directory

1. In Cellebrite Commander select **Configurations > By product**. The following window appears.

Product configuration  
UFED Products  
Configuration template: UFED master template - Anna's  
Template last publication: 26/09/2020 01:00  
Duplicate template Delete template EDIT PUBLISH

General

Application language	English
Additional languages	English, Arabic, Chinese, Croatian, Czech, Dan..., French, German, Italian, Japanese, Korean, Portuguese, Spanish, Turkish
Additional report languages	English, Arabic, Chinese, Croatian, Czech, Dan..., French, German, Italian, Japanese, Korean, Portuguese, Spanish, Turkish
Prompt for confirmation on exit	Off
Show virtual keyboard	Off
Enable access to connectivity settings	Off
Include Case Details	On
Include Camera screen	On
Min. number of pictures/videos	100

2. Click **Edit**, to enable the following under the Access Control section:
  - a. **Require login**.
  - b. **Enable Active Directory integration**.

3. Under **Permissions level**, select one of the following options:

- » **Active Directory groups:** Manage permissions at the Active Directory groups level. The match is performed by Active Directory group names.
- » **Active Directory users with Commander roles:** Manage permissions per user independently from Active Directory groups.

4. Click **Save** to save the configuration template.

5. Publish the configuration template to the relevant product.

Next you need to add the Active Directory profile and select the required permissions.

#### 4.9.1.4.1. To add a role and select permissions

Adding roles and selecting permissions are managed in the User Management System. For more information, see the Managing Roles section in the User Management System manual.

#### 4.9.1.4.2. Adding Users

Adding users is managed in the User Management System. For more information, see the Managing Users section in the User Management System manual.

#### 4.9.1.5. Logging in to Cellebrite UFED

Once Active Directory is enabled, the following will occur depending on the Cellebrite UFED device you are using.

- » In PC applications such as Cellebrite UFED 4PC and Cellebrite Responder, the login will occur automatically when you start the Cellebrite UFED application.
- » In closed systems such as Cellebrite UFED Touch and Kiosk, Cellebrite UFED tries to locate the domain and display the following login screen.



1. Enter the Active Directory credentials.
2. Verify the Domain field.



If the text in the “Domain” field (i.e., “domain controller host”) is missing or incorrect, contact your IT department.

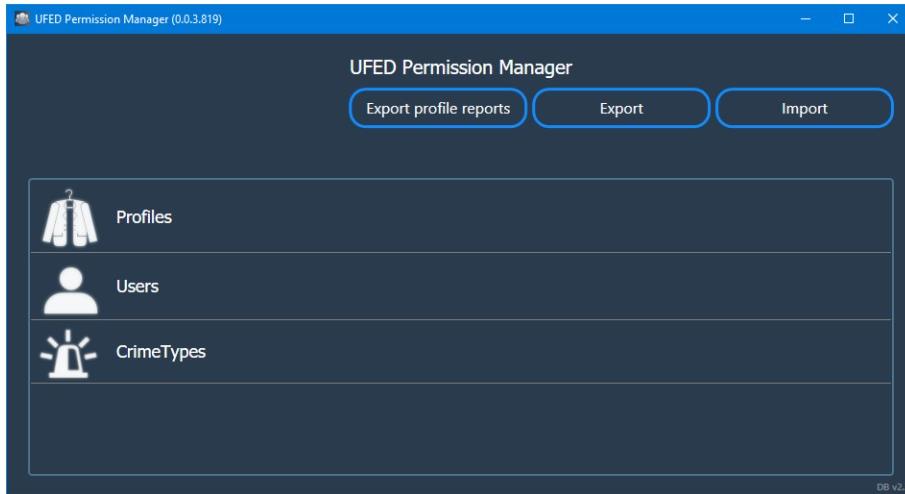
#### 4.9.1.6. Cellebrite UFED Permission Manager

If you are not using Cellebrite Commander, use the following procedures in the Cellebrite UFED Permission Manager and Cellebrite UFED application to enable Active Directory.

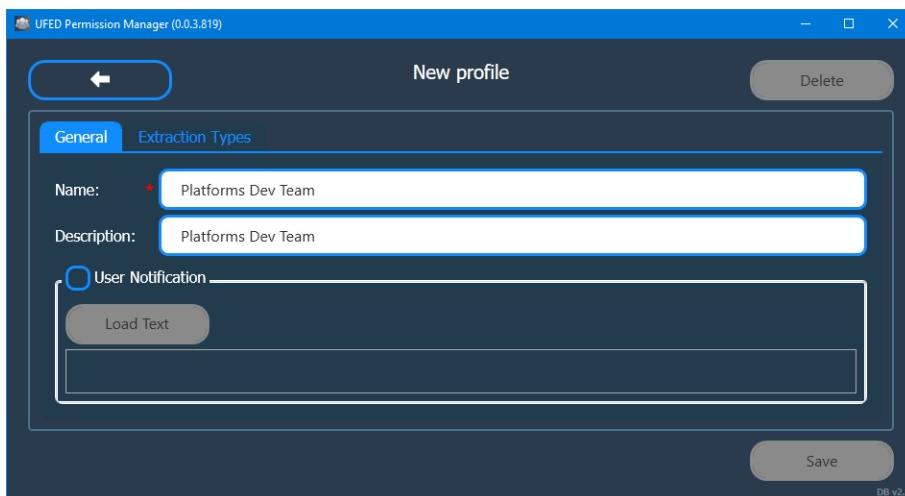
##### To configure Active Directory in the Cellebrite UFED Permission Manager:

In the Cellebrite UFED Permission Manager, create a profile that corresponds to the required Active Directory group.

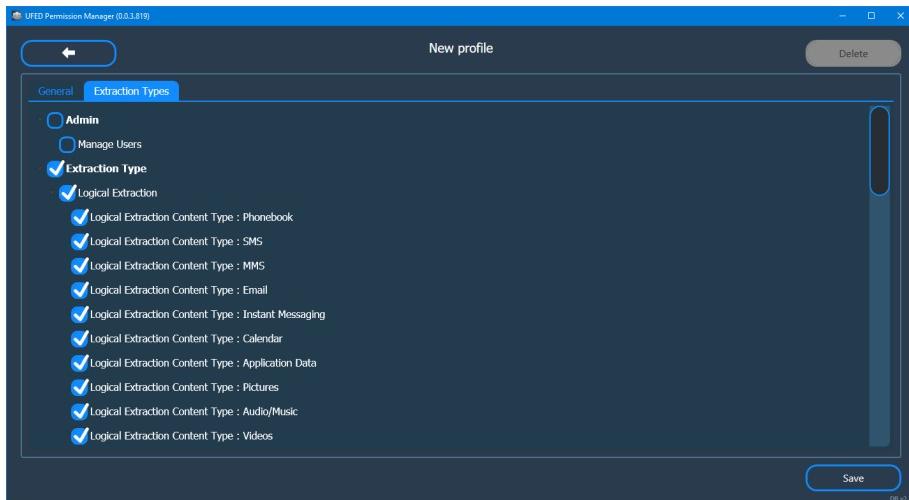
1. Run the Cellebrite UFED Permission Manager. The following window appears.



2. Click **Profiles** > **New Profile**. The following window appears.



3. In the Name field enter the name of the Active Directory group. i.e., Platforms Dev Team.
4. Enter a description (optional).
5. Click **Extraction Types** and enter all the required permissions for the profile. The following window appears.



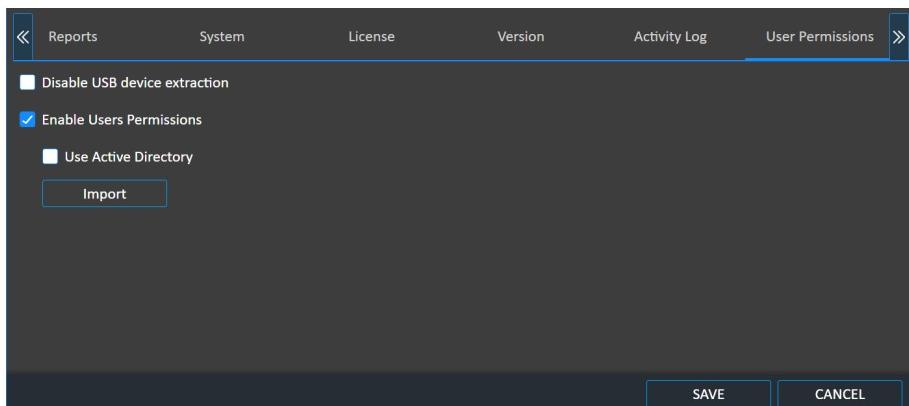
6. Click **Save**.

**To enable Active Directory in the Cellebrite UFED application:**



This step is not required if you are using Cellebrite Commander.

1. In Cellebrite UFED go to **Settings > User Permissions**.



2. Select **Use Active Directory**.



You can only login to the application using Active Directory users, there will no longer be Cellebrite UFED users such as Manager and Investigator. After activating Active Directory either in Cellebrite Commander or Cellebrite UFED application.

3. Click **Save**. The following window appears.

### Notice

For the change to take effect, you must restart or log in to the application again.

OK

- Click OK and restart the Cellebrite UFED application.

For information on how to login to the Cellebrite UFED devices, see [Logging in to Cellebrite UFED \(on page 98\)](#).

## 4.9.2. Permission management

Permission management can be performed via Cellebrite Commander or the Cellebrite UFED Permission Manager standalone application.

The Cellebrite UFED Permission Manager standalone application is available from [MyCellebrite](#). Each profile contains access permissions, including operation rights per extraction type and content types. A single profile can be assigned to multiple users. The users and profiles can be exported into an encrypted permission management file, which can be imported into multiple Cellebrite UFED applications.

### 4.9.2.1. Using the Cellebrite UFED Permission Manager

To create a new profile:

- Download the latest Cellebrite UFED Permission Manager application from your account in [MyCellebrite](#), and save it to a directory on a computer or external device.
- Run the Cellebrite UFED Permission Manager and follow the setup instructions. The Cellebrite UFED Permission Manager screen appears.



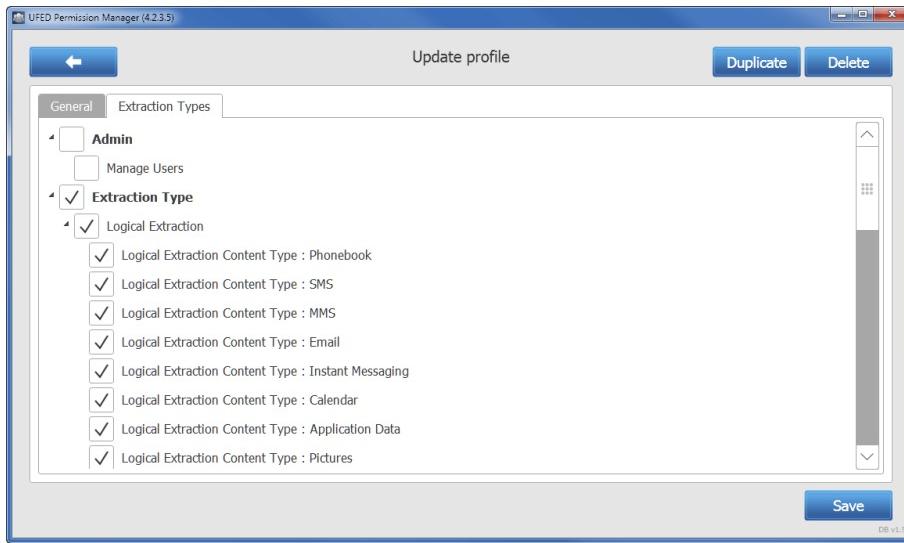
- Click Profiles.



4. Click **New Profile**. The following screen appears.



5. Enter a name and description for this profile.
6. If required select the **User Notification** check box, which enables you to load a RTF file with text and graphics for the profile.
7. Click the **Extraction Types** tab.



- Select the options for this profile, such as Admin who can manage users, the Extraction Type (Logical Extraction, SIM Data extraction, Password extraction etc.) and UFED Settings (Activity Log).

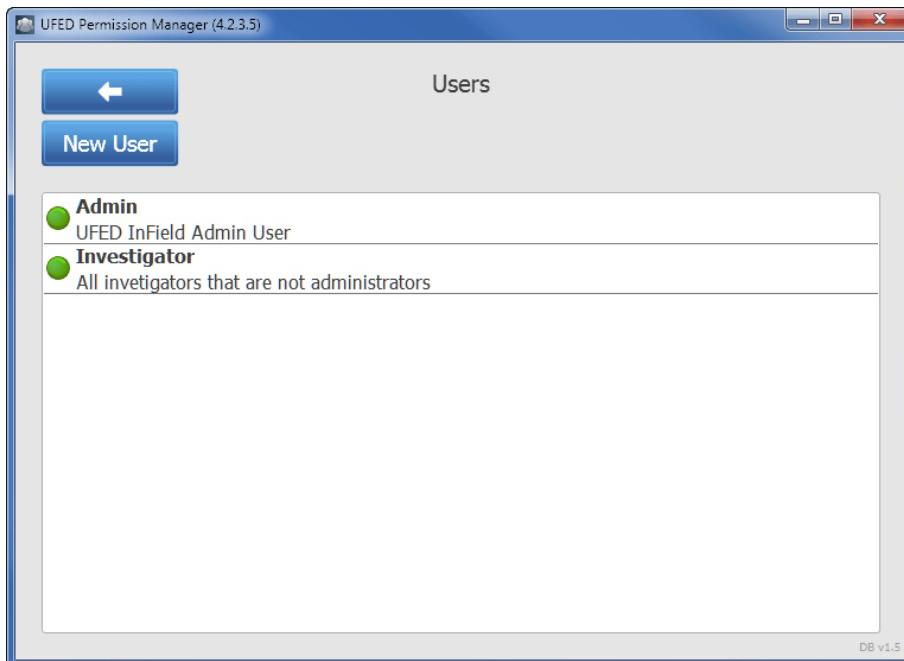


At least one of the enabled users must be an Administrator (Admin).

- Click **Save** and proceed to create a new user.

#### To create a new user:

- In the Cellebrite UFED Permission Manager screen, click **Users**. The following screen appears.



- Click **New User**. The following screen appears.

The screenshot shows the 'New user' dialog box from the UFED Permission Manager. It contains the following fields:

- Username: Required field
- Display Name: Required field
- Description: Text input field
- Password: Required field, with validation message: "Password must contains at least 8 characters."
- Confirm Password: Required field, with validation message: "Password must contains at least 8 characters."
- Profile: Drop-down menu
- Enabled?: Checkbox

Buttons at the bottom include 'Save' and 'Delete'.

- Enter the details for the new user including Username, Display Name, Description, and Password.
- Select a profile for the user.
- Select **Enabled** to enable the user.
- Click **Save**.

### To manage crime types:

- Click **Crime Types**. The following screen appears.

The screenshot shows the 'Crime Types' dialog box. It lists the following crime types:

- Armed Robbery
- Attempted Murder
- Child Exploitation
- Child Molest
- Child Pornography
- Counterfeiting
- Crime Confinement

Buttons at the top include 'New Crime Type' and 'Delete all crime types'.



The crime types are only relevant for Cellebrite Responder.

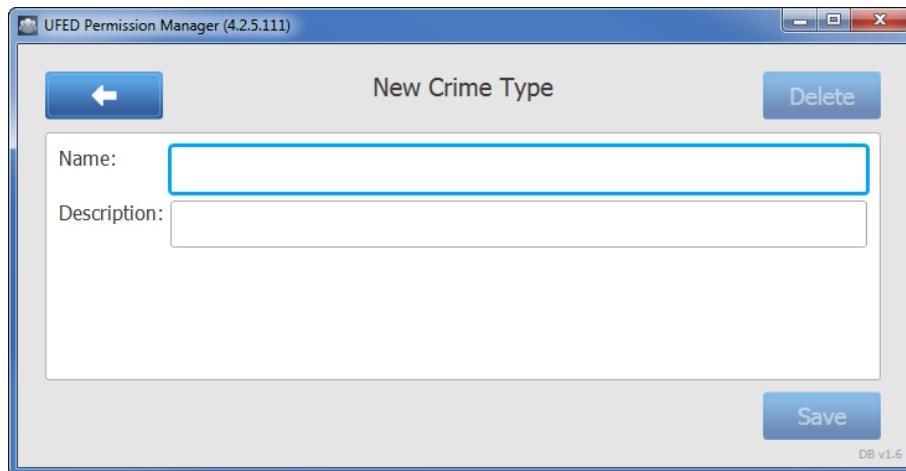


You can delete all crime types; however you must add at least one crime to be able to export a permission management file.



To edit a crime type, click the crime type and edit the Name.

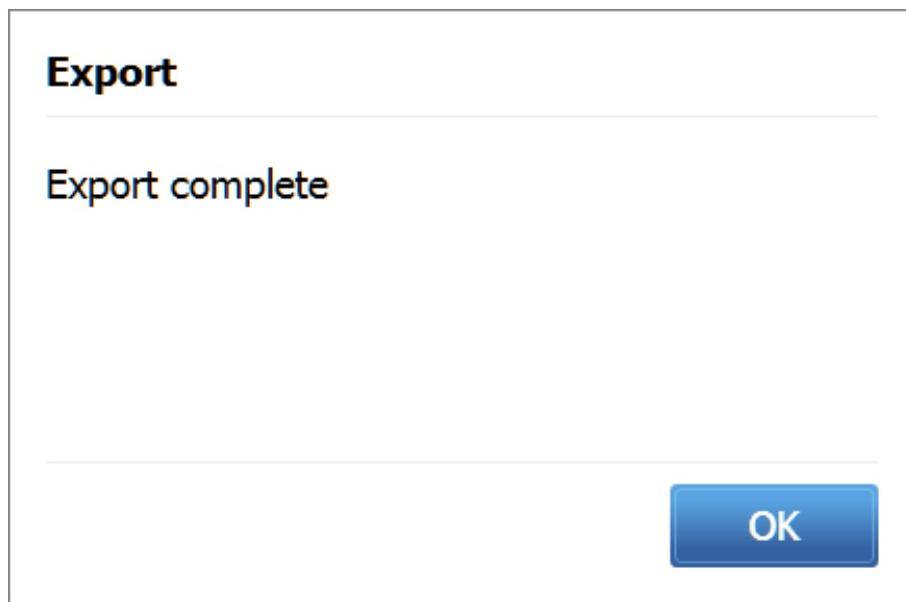
2. Click **New Crime Type**. The following window appears.



3. Enter a name for the crime type and a description (optional).
4. Click **Save**.

**To export an encrypted permission management file:**

1. In the Cellebrite UFED Permission Manager screen, click **Export**, specify a directory for the file and click **Save**. The following screen appears.



2. Click **OK**. The permission file must be imported into Cellebrite UFED via the User Permissions tab in the Settings window.



The next time you run the Cellebrite UFED Permission Manager you will be prompted for your user credentials to access the application.

## 5. Special cables

Cellebrite UFED requires a special cable for certain functions as follows:

[Device power-up cable \(below\)](#)

[Active extension cable \(on the next page\)](#)

[USB extension cable \(on the next page\)](#)

[USB cable for Cellebrite UFED Device Adapter V2 PowerUP \(on page 108\)](#)

### 5.1. Device power-up cable

In case of a drained or absent battery, the device power-up cable powers the device instead of the battery while performing an extraction.

The device power-up cable contains four parts marked as: Data, Extra power, "-", "+".



Phone power-up cable

#### To connect the device power-up cable:

1. Connect the Extra Power connector to the Cellebrite UFED USB Port extension.
2. Connect the Data connector to the Cellebrite UFED USB Port extension.
3. Identify the device's battery contacts:
  - » Open the device battery cover.
  - » Locate the positive ('+') and negative ('-') pole markings of the battery, usually found next to the contacts area.
  - » Make sure that the battery contacts are marked clearly on the device's body.
  - » Remove the battery in order to gain access to the device's battery contacts.

**TIP:** For battery contacts which are not clearly marked on the device's body, use the pole markings on the battery body to identify them. To do that, simply flip the battery along its contacts edge, and place it along the edge of the battery housing, then mark the device's contacts according to those on the battery.



Use a multi-meter to identify the positive and negative poles of an unmarked battery.

4. Connect the **RED** alligator clip to the device's positive pole ('+'), the Primary **Black** alligator clip to the negative pole ('-') and the secondary **Black** alligator to middle pole in case of three poles or to the one next to the (-) in case of four poles. Make sure the alligator clips are not closing a circuit by touching each other.
5. Connect the source device to the **phone power-up cable** using the references cable from the cable organizer kit as listed in the Cellebrite UFED menu.

## 5.2. Active extension cable

This cable is 150 cm in length and allows for the easy and accessible placement of the Cellebrite UFED Device Adapter with USB 3.0. For more information on the adapter, see [Cellebrite UFED Device Adapter with USB 3.0 \(on page 11\)](#).

The USB Device Adapter Active extension cable is a custom made, high grade cable with an active USB 3.0 extension. It is a bus-powered extension cable that can be used to increase the length of the Cellebrite UFED Device Adapter without any signal loss or performance issues. It contains active electronics, which boost the USB signal for maximum reliability and performance over extended distances.



The previous USB extension cable i.e., "USB Extension cable for Cellebrite UFED Device Adapter" cable should only be used with the Cellebrite UFED Device Adapter with USB 2.0.

## 5.3. USB extension cable

This USB extension cable is 150cm in length and will allow for the easy and accessible placement of the Cellebrite UFED Device Adapter V2. In a desktop environment where the computer is mounted in a difficult to access or distant location the USB Extension cable should be used.

The USB Extension cable is a custom made high grade cable. This high grade cable prevents voltage fluctuation and is shielded from EMI interference which would cause signal degradation or loss.

If an extension cable is needed it is **essential** that the provided USB Extension cable is used. Use of third-party cables will affect performance of your Cellebrite UFED and may prevent some functions from starting or completing.

## 5.4. USB cable for Cellebrite UFED Device Adapter V2 PowerUP



The following USB PowerUP cables are applicable to the Cellebrite UFED Device Adapter V2. These cables are **no longer required** with the Cellebrite UFED Device Adapter V3.

- » The **USB Cable for Cellebrite UFED Device Adapter PowerUP S** for use with your Cellebrite UFED. It is 75cm in length.
- » The **USB Cable for Cellebrite UFED Device Adapter PowerUP L** for use with your Cellebrite UFED. It is 150cm in length.

Both cables provide the same functionality and differ only in length.

The PowerUP cable has a miniUSB male end which will plug into the Cellebrite UFED Device Adapter V2 and a USB-A connector which can be plugged into any available powered USB port - including A/C powered USB chargers and car chargers.

The PowerUP cable will double the power capacity of the Cellebrite UFED Device Adapter V2. This will ensure that all devices with excess power requirements will function correctly and will allow Cellebrite UFED to provide all functions. In addition devices that are fully discharged may need the additional power that the PowerUp cable will provide.

In the laptop environment it is recommended that the PowerUp cable is used when Cellebrite UFED indicates that the extra power is needed.



The PowerUp cable is NOT required for smooth operation of the Cellebrite UFED for most devices, but is provided for those cases where power consumption is above the capacity of the unpowered Cellebrite UFED Device Adapter V2.

## 6. Regulatory compliance

Part	Cellebrite UFED Standard and Ruggedized
CE	
EMC	EN 301 489-1 EN 301 489-7 EN 55024
Safety	IEC/EN 60950-1
Radio frequency spectrum usage	EN 300 328 V2.1.1
FCC	
EMC	FCC part 15, subpart B
Radio	FCC part15.247

## 7. Specifications: Cellebrite UFED Device Adapter



The specifications for the **UFED Device Adapter**<sup>1</sup> with USB 3.0 are subject to change without notice.

Item	Properties	
Power	USB Powered Optional additional power connection from external 5.3V power supply	
Dimensions	67.9mm (D) x 115.8mm (W) x 24.6mm (H)	
Weight	200 g	
Bluetooth	V2.1+EDR (Backward compatible with V1.1/V1.2/V2.0)	
USB	Device: 1 x USB 3.0	
	<b>Connection type</b>	<b>Power capabilities</b>
	USB2.0 single port	300 mA
	USB2.0 dual port	800 mA
	USB3.0 single port	600 mA
	USB3.0 dual port	900 mA
	External Power Supply	2800 mA
Host Interface: 1 x USB 3.0 port		
Serial ports	RJ-45 for device connectivity	
Environmental	Operating temperature: 0°C – 40°C Storage temperature: -20°C – 60°C	

---

<sup>1</sup>The Cellebrite UFED kit contains a device adapter that attaches to your PC's USB ports. Each connector has a LED that indicates availability during an extraction and blinks to indicate where to connect the source device. In addition, there are LEDs for power and Bluetooth. Depending on when you received your Cellebrite UFED kit, there are two types of device adapters: Cellebrite UFED Device Adapter with USB 3.0 (latest version) and Cellebrite UFED Device Adapter with USB 2.0 (previous version).

Item	Properties	
	Part	Description
	CE	This device complies with the essential requirements of <b>RED Directive 2014/53/EU</b> 2014/35/EU 2014/30/EU
		Following standards: EN 301 489-1
Regulatory compliance	EMC	EN 301 489-17 EN 55024
	Safety	IEC/EN 60950-1, CB Scheme
	Radio frequency spectrum usage	EN 300 328
	FCC	
	EMC	FCC part 15, subpart B
	Radio	FCC part 15.247

## 7.1. Specifications: Multi SIM Adapter



The specifications are subject to change without notice.

Item	Properties	
Power	USB Powered	
Dimensions	61.6mm [D] x 56.3mm [W] x 15.5mm [H]	
Weight	80 g	
Interfaces	<p>Host Connection: 1 x USB 2.0 port Integrated SIM card reader supporting the following SIM cards: Micro SIM Nano SIM Standard SIM</p>	
Environmental	<p>Operating temperature: 0°C – 40°C Storage temperature: -20°C – 60°C</p>	
Regulatory compliance	Part	Description
	CE	EN 301 489-1
	EMC	EN 301 489-7 EN 55024
	Safety	IEC/EN 60950-1
	EMC FCC	FCC part 15, subpart B

## 8. Ordering cables and accessories

If you have a valid Cellebrite UFED 4PC license, it is possible to request missing cables and accessories in the MyCellebrite portal.

Customers can request up to two cables from each cable type per year at no charge.

Once ordered, you will receive a confirmation that your request has been accepted, and a notification when shipped.

### To order cables and accessories:

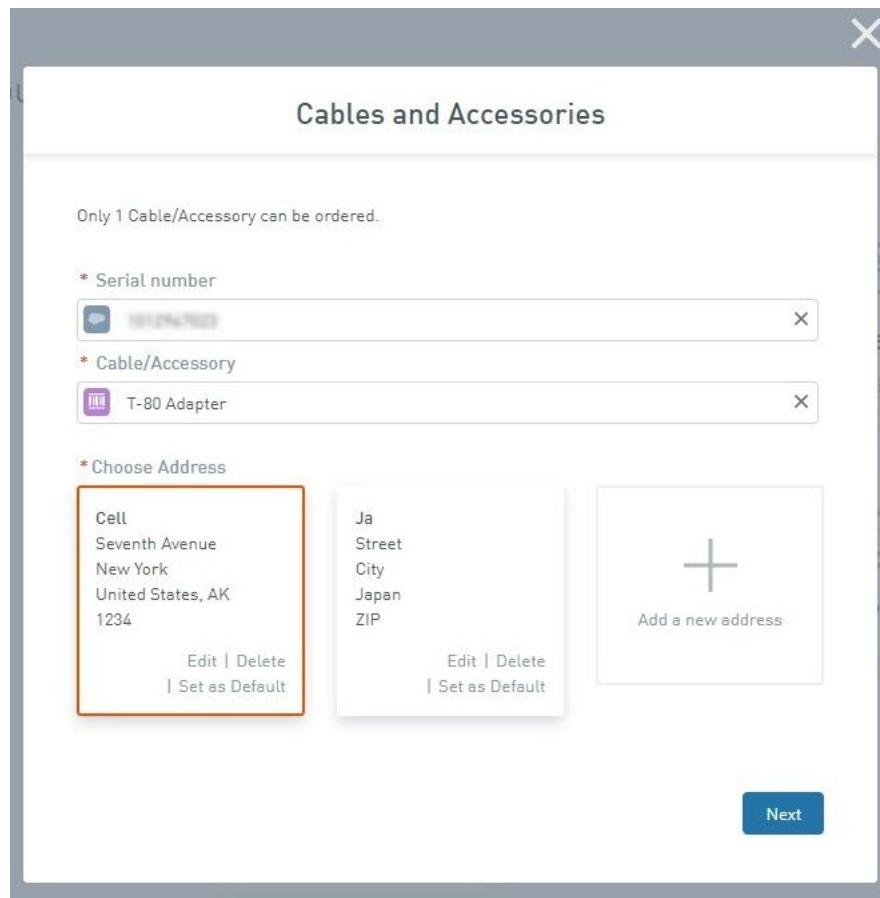
1. Go to the [MyCellebrite portal](#).
2. Navigate to **Support > Manage Tickets**.
3. Click **+ New Ticket**.

The screenshot shows the 'Support Requests' section of the MyCellebrite portal. At the top, there are navigation links: HOME, PRODUCTS & LICENSES, SUPPORT (which is highlighted in red), ADVANCED SERVICES, STORE, and MORE. Below the navigation is a search bar with a dropdown menu labeled 'Status Filter' set to 'Open' and a search input field. To the right of the search bar is a red button labeled '+ New Ticket'. A small orange circle with the number '9' is positioned in the top right corner of the main content area. The main content area displays a table with columns for Action, Date Created, Case Number, Case Subject, and Case Status. A message 'No records' is centered below the table. At the bottom of the page, there is a footer with the MyCellebrite logo, copyright information, and privacy notice links.

4. Click **Cables & Accessories**.

The screenshot shows the support categories page of the MyCellebrite portal. At the top, there are navigation links: HOME, PRODUCTS & LICENSES, SUPPORT (highlighted in red), ADVANCED SERVICES, STORE, and MORE. Below the navigation is a search bar with the placeholder 'How can we help you?'. The page features six service categories arranged in a grid: 'Technical Support' (icon of a speech bubble with a gear), 'Cables and Accessories' (icon of a coiled cable), 'Defective Device Replacement' (icon of a cube with a gear), 'Trial' (icon of a stopwatch), 'Sales Inquiry' (icon of a shopping cart), and 'Training Support' (icon of a graduation cap). The 'Cables and Accessories' category is highlighted with a red border around its icon and text. At the bottom of the page, there is a 'CAS Support' section featuring a logo with the letters 'CAS' and a small gear icon.

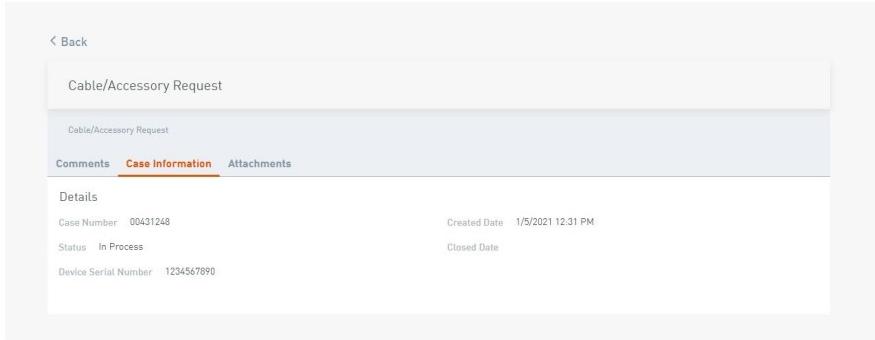
5. Enter the serial number for the product.
6. Select the cable or accessory.
7. Select or add a new address.
8. Click **Next**.



9. Click **Next**.



10. The case details are displayed.



11. Once the cables are shipped you will receive an email notification with the tracking number.
12. You can view the case and its status any time in the MyCellebrite portal by going to **Support > Manage Tickets**:

Action	Date Created	Case Number	Case Subject	Case Status
Case Details	Jan 5, 2021	00431247	Cable Request	In Process
Case Details	Jan 5, 2021	00431246	RMA Request - wr6tf	New
Case Details	Jan 4, 2021	00431240	RMA Request	In Process
Case Details	Jan 4, 2021	00431239	Cable Request	In Process
Case Details	Jan 4, 2021	00431238	RMA Request	In Process
Case Details	Jan 4, 2021	00431237	Cable Support	New

## 9. Glossary

---

### A

---

#### Active extension cable

This cable is 150 cm in length and allows for the easy and accessible placement of the UFED Device Adapter with USB 3.0.

#### ADB

Refers to an extraction method most commonly used for file system extractions.

ADB, AKA Android Debug Bridge, is a built-in communication mechanism originally designed for device debugging. To enable the device extraction, ADB must be turned on.

#### ADB (Rooted)

When extracting a rooted device, the operating system version is not a limitation and the extraction can be completed on any Android version.

#### Advanced ADB

Refers to a physical extraction method, where ADB is used to facilitate the extraction. This method is available for Android OS versions created before December 2016. Depending on the device, this extraction may perform faster than other extraction methods, but takes considerably longer than other extraction methods. With this extraction type, the source device will continue the extraction, once the appropriate commands are sent to the device, with the output directed towards a USB mass storage device (via OTG cable) or SD memory card.

#### Advanced ADB (Generic)

This process is similar to the ADVANCED ADB mentioned however it is not verified for use on a specific device. It has however been shown to be successful on many

---

similar devices. In some rare cases, it may not perform as expected, therefore, we recommend trying other extraction types first.

### Advanced logical extraction

An extraction method that combines both the logical and file system extractions into a single extraction method. This method helps users overcome the pain of long and convoluted extractions, saving time and effort while maintaining forensically sound data.

### Airplane mode

Flight mode, Offline mode, or Standalone mode is a setting that when activated it disables all voice, text, telephone, and other signal-transmitting technologies such as Wi-Fi and Bluetooth. Wi-Fi and Bluetooth can be enabled separately even while the device is in airplane mode.

### Allocated space

The area on a device's memory that stores data in an organized manner, and contains its operating system and user data. Logical extractions obtain data from allocated space only.

### Android Backup

Supports Android devices running OS version 4.1 and later. It typically provides less data than a regular "ADB" backup, however, depending on the make, model and OS version of the device, it may be the only option available or can be used when the ADB option exists, but is not successful.

### Android Backup APK Downgrade extraction

This method focuses on specifically supported apps for decoding. It should be used as a last resort method as data alteration will occur during this process. This method temporarily downgrades the updated version of the app on the device and installs the latest supported version of the app that it can decode.

---

## apk

Android application package file. Each Android application is compiled and packaged in a single file that includes all of the application's code (.dex files), resources, assets, and manifest file.

## Apple File Conduit

AFC2. A service that is used by computer applications such as iTunes and iPhoto to read files from a device over USB.

---

## B

### Boot loader

A small piece of code that is inserted into the RAM during start-up. In the commercial wireless world, this allows flashing of firmware. In the forensic world, it allows a non-intrusive means of accessing and copying user data into a forensic image.

### Brick

A device that cannot function in any capacity (such as a device with damaged firmware).

### Bruteforce

Refers to an unlocking technique that relies on trial and error. Combinations are attempted until the correct password or PIN is found.

---

## C

### CAS

Cellebrite Advanced Services (CAS) offers customers the ability to recover valuable evidence from heavily damaged, locked or encrypted devices.

---

## CDMA

Code Division Multiple Access. These networks connect using different methods to allow multiple callers access to single voice radio waves, hence Code and Time Division. True CDMA networks do not require handsets to have a SIM card, as the network connects to the device and the subscriber details are contained in the handset rather than a SIM card.

## Cellebrite Commander

Simplify how you manage and control all deployed devices and systems with the Cellebrite Commander. Reduce ongoing administration costs by remotely accessing devices and systems across your operation.

## Cellebrite UFED 4PC

Enables users to deploy extraction capabilities on Windows based tablets, laptops, and desktop computer systems. It performs physical, logical, file system and password extractions on a wide range of devices.

## Cellebrite UFED Device Adapter

The Cellebrite UFED kit contains a device adapter that attaches to your PC's USB ports. Each connector has a LED that indicates availability during an extraction and blinks to indicate where to connect the source device. In addition, there are LEDs for power and Bluetooth. Depending on when you received your Cellebrite UFED kit, there are two types of device adapters: Cellebrite UFED Device Adapter with USB 3.0 (latest version) and Cellebrite UFED Device Adapter with USB 2.0 (previous version).

## Cellebrite UFED Touch

Enables the simplified extraction of mobile device data. Depending on the license purchased, it performs physical, logical, file system and password extractions on a wide range of devices.

---

## Chip-off

Obtain data straight from the mobile device's memory chip. The chip is detached from the device and a chip reader or a second device is used to extract data stored on the device under investigation.

---

## D

### Decrypting Bootloader

This process is designed for Android devices that have Qualcomm chipsets. This extraction can be performed when the device is in Bootloader mode. Bootloader extractions do not support extractions from a memory card or SIM card.

### Device power-up cable

In case of a drained or absent battery, the device power-up cable powers the device instead of the battery while performing an extraction. The device power-up cable contains four parts marked as: Data, Extra power, "-", "+".

### Dongle license

Is a software copy protection device that plugs into the USB port of the computer. Upon startup, the application looks for the key and will run only if the key contains the appropriate code.

---

## E

### EDL (Emergency Download)

Included in the cable or tip set received with your UFED, is an EDL cable. The EDL method is sometimes a superior alternative to advanced techniques, such as JTAG, ISP and Chip-off as they typically can be accomplished without advanced or invasive techniques. It's also possible to use this method on devices that do not function due to damage.

---

## Extraction

The process of obtaining mobile device data and storing it in an approved location for processing.

## Extraction files

Files used to capture forensic evidence from mobile devices. This includes mobile phones, handheld tablets, portable GPS devices, and devices manufactured with Chinese chipsets. Extraction types include Logical, SIM Password, File system, physical, capture images, and capture screen shots. Extraction files: MSAB Extended XML, XLS, XLSX, XMK, CSV, TXT, UFD, UFDR, CDR

---

## F

### Facelock

Uses an image of the user captured by the front camera to unlock the device. There must be some movement in the face when unlocking the device, to prevent someone from using a still photo to gain access.

### File system extraction

Obtains files embedded in the memory of a mobile device. Retrieve the artifacts within a Logical extraction, in addition to hidden system files, databases and other files which were not visible within a logical extraction.

### Fingerprint

Newer devices have a fingerprint sensor built into the home button. The user places their finger upon the sensor to gain access to the device.

### Forensic Recovery Partition

This extraction method will perform a physical extraction while the device is in Recovery mode. With this extraction method, the original recovery partition is replaced with Cellebrite's custom forensic recovery partition. Using Cellebrite's

---

custom forensic recovery partition does not affect any of the user data, is forensically sound, and will bypass the user lock from a number of Samsung Android devices.

## Forensically sound

Extracted data is said to be forensically sound if it was collected, analyzed, handled, and stored in a manner that is acceptable by the law, and there is reasonable evidence to prove so. Forensic soundness provides reasonable assurance that extracted data was not corrupted or destroyed during investigative processes, whether on purpose or by accident.

## I

---

### ICCID

Integrated Circuit Card Identifier. GSM identifier

### IMEI

International Mobile Equipment Identifier. GSM identifier

### IMSI

International Mobile Subscriber Identity. GSM identifier

### Iris scan

Different from retina scans, an iris scan is a form of biometric identification using iris pattern-recognition techniques. The owner of the device establishes the security feature by video scanning the complex, unique but stable patterns of the eye portion surrounding the pupil.

## J

---

### Jailbreaking

A jailbroken iOS device or a rooted Android device is one whose owner has taken steps to bypass its factory settings, including built-in security and other restrictions. Jailbreaking an iOS device allows the user to install third-party apps from sources

---

other than the App Store, while rooting an Android device provides administrative “root” access to its operating system. UFED solutions do not rely on jailbreaking or permanent rooting to perform forensic extractions, as other mobile forensic tools do.

## K

---

### Knock pattern

The user taps certain locations on the screen in a certain order to gain access to the device.

## L

---

### Logical extraction

Extracts user data from a mobile device (SMS, call logs, pictures, phonebook, videos, audio, certain application data, and more). Quickest extraction method but least amount of data.

## M

---

### MEID

Mobile Equipment Identity (MEID) is the CDMA equivalent of the International Mobile Equipment Identifier (IMEI) for Global System for Mobile communications (GSM) handsets and is often referred to as the serial number of the handset.

### MIN

Mobile ID Number (MIN) is often compared to the International Mobile Subscriber Identity (IMSI) found associated to GSM handsets. The MIN is the number which identifies the subscriber to the CDMA network provider.

### MSISDN

Mobile Station International Subscriber Dialing Number. GSM identifier.

---

## **MultiSIM Adapter**

Is a small-size adaptor which enables reading, data extraction and cloning Nano SIM, Micro SIM and SIM cards.

---

## P

---

### **Password Lock/Bypass**

Users of devices are routinely secure their data with the use of password locks and security measures. The bypassing or discovery of these security measures largely depends on the make and model of the device as well as the operating system that is in use. Using Cellebrite's extraction technology, some devices are able to have bypasses, where a series of specialized cables and instructions are supplied to either bypass or defeat a security mechanism used. In other cases, instructions will be provided which will allow the user to have the PIN/PASSCODE displayed on the screen.

### **Physical extraction**

The most comprehensive extraction and forensically sound. It uses advanced methods to extract a physical bit-for-bit image of the flash memory of a device, including the unallocated space. Unallocated space is the area of the flash memory that is no longer tracked by the file system. Unallocated space may contain images, videos, files, and more.

### **Physical/Logical Analyzer**

An analysis and reporting tool for logical, file system and physical extractions. This software solution provides users with the capability to extract data, perform advanced analysis, decoding and reporting and presenting the results in a clear and concise manner.

### **PIN/Password and Pattern Lock**

All of the above locks require a secondary lock such as a PIN, password, or pattern lock. Also, a user may select one of these as the primary screen lock for their device.

---

## R

---

### Root

A process that allows users of cell phones and other devices running the Android operating system to attain privileged control (known as "root access") within Android's Linux subsystem, similar to jailbreaking on Apple devices running the iOS operating system, overcoming limitations that the carriers and manufacturers put on such devices.

---

## S

---

### Selective extraction

Performs fast and focused extractions. Pick and choose the applications in which you suspect contains relevant data or leads, and perform a Selective extraction rather than waiting several hours for a full file system extraction.

### Smart ADB

This method is designed for Android devices that include the "November 2016" security patch. It is supported by OTG compatible devices with OS versions 6.0 and above. Only security unlocked devices are supported.

### Smart location

Trusted locations leave the device unlocked for up to four hours when it is turned on, and the device is connected to a secured Wi-Fi access point, trusted Bluetooth device, trusted NFC tag, or if the device detects body movement.

---

## T

---

### TAC

The Type Allocation Code (TAC) is the initial eight-digit portion of the 15-digit IMEI and 16-digit IMEISV codes used to uniquely identify wireless devices. The Type

---

Allocation Code identifies a particular model (and often revision) of wireless telephone for use on a GSM, UMTS or other IMEI-employed wireless network.

## U

---

### UFD

Once logical, file system, and physical extractions are complete, UFED generates an extraction file, along with a .UFD (text) file. The .UFD file contains information about the extraction, such as which UFED was used (including its serial number); start time, finish time, and date; and hash information. With iOS physical extractions, the .UFD file also contains decryption keys. For binary images, it may contain some information to aid the decoding process.

### UFDR

Universal Forensic Extraction Device Report

### UFDX

UFED generates a UFDX file when there are multiple extractions for a device. It contains information about each extraction

### UFED

Universal Forensic Extraction Device

### UFED CHINEX

The UFED Chinex kit, is the solution to complete a physical extraction, decoding of evidentiary data and passwords from mobile devices manufactured with Chinese chipsets; including MTK and Spectrum.

### UFED kit

The UFED kit includes connection cables and tips. These are used to connect mobile devices to UFED.

---

## UFED Memory Card Reader

A multi-format card reader that provides either read-only or read-write access to a variety of flash media cards.

---

## V

---

### Voice lock

The user speaks while unlocking the device, and their voice gains access.

# 10. Index

- Clone SIM 9  
Console, Android Debug 29, 50
- A**
- Accessories 10, 113
  - Activating the license 21
  - Active Directory 93
  - Activity log 89
  - Activity Log 103
  - Android backup 20
  - APK for Android backup APK downgrade 20
  - Application taskbar 36
  - Autodetecting 28
- C**
- Camera checklist, importing 85
  - Camera screen, enabling 60
  - Capture 9
  - Capture images 9
  - Capture images and screenshots 10
  - Case details 37
  - Case details, importing 86
  - Cellebrite YouTube channel 15
  - Changing the application interface language 60
  - Changing the extraction location 64
- D**
- Device power-up cable 106
  - Dongle 21, 26, 75
  - Dongle license 21
- E**
- Export options 69, 84, 89, 91, 104
  - Extractions, [Refer to Performing extractions in MyCellebrite] 9, 49, 99, 102
- F**
- File system extraction 9
  - file system extractions, timeframe options 33
- G**
- Files, logical extraction type 52
- H**
- General settings 50, 57
  - Getting started 16
- I**
- Home screen 27, 37, 54, 74, 76
  - IMEI, search 30
  - Importing settings and configuration files 84
  - Interface language 57, 60
  - Investigation notes 38

**L**

Legal notices 2  
license not found 71  
License settings 70  
Logging in 98  
Logical extraction 7, 9-10, 14, 49, 60, 103

**M**

Managing report fields 67

**N**

Network 26  
Network dongle 25

**O**

Overview 1, 7, 12, 49

**P**

Password extraction 9, 103  
Performing extractions 29, 50  
Permission management 101

Permission Manager 37, 92, 96, 101  
Permissions  
Users 92

Physical extraction 9

**R**

Regulatory compliance 109  
Report settings 65

**S**

Screenshots 10, 39  
Searching for a device 30  
Select content types 14  
Selective extraction 33-34  
Settings 20, 33, 37-38, 56, 62, 65, 79, 82, 90-91, 100, 103

SIM extraction 9

Simplified Chinese 63

Sounds, play notifications 69

Special cables 106

Specifications 2, 12, 110, 112

Specify a network location 110, 112

Starting the application 26

Supported devices 14

System requirements 8

System settings 51, 69

**T**

TAC number search 31

**U**

UFED Device Adapter 11, 13, 107-108, 110

Unallocated space 9

Update via the web 79

Updates and versions 79

User permissions 92

User predefined filter 33

Using cables and tips 14

V

Version details 79